Name: Irfan Kamate
USN: 2GI19CS052

Assignment-1

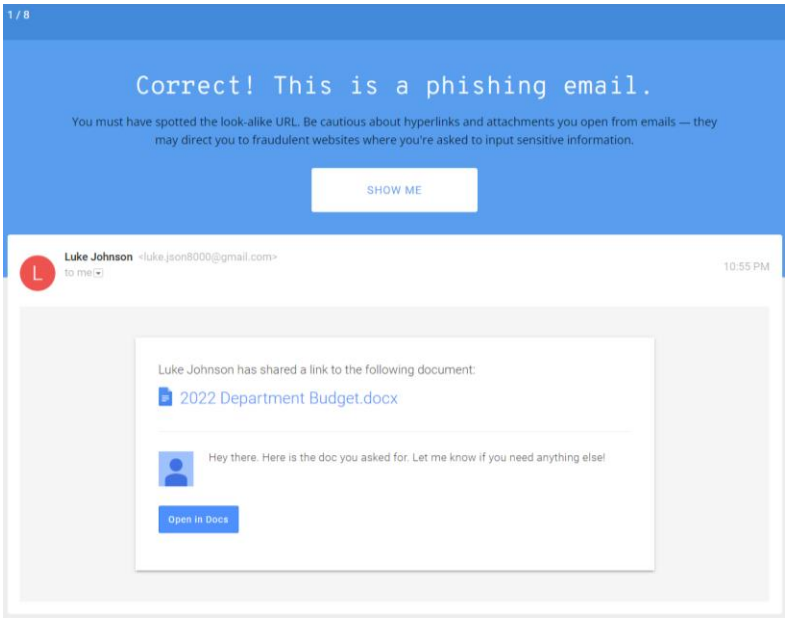
Activity - 1

Task: Identify the following mails are “Phishing” or “Legitimate”

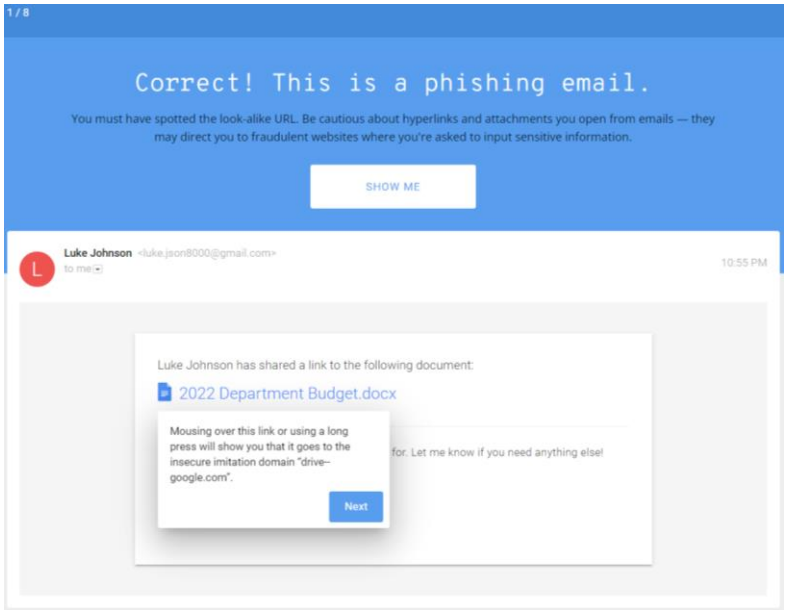
Phishing: an attack that attempts to steal your money, or your identity, by getting you to reveal personal information - such as credit card numbers, bank information, or passwords - on websites that pretend to be legitimate.

Legitimate: something legal or acceptable.

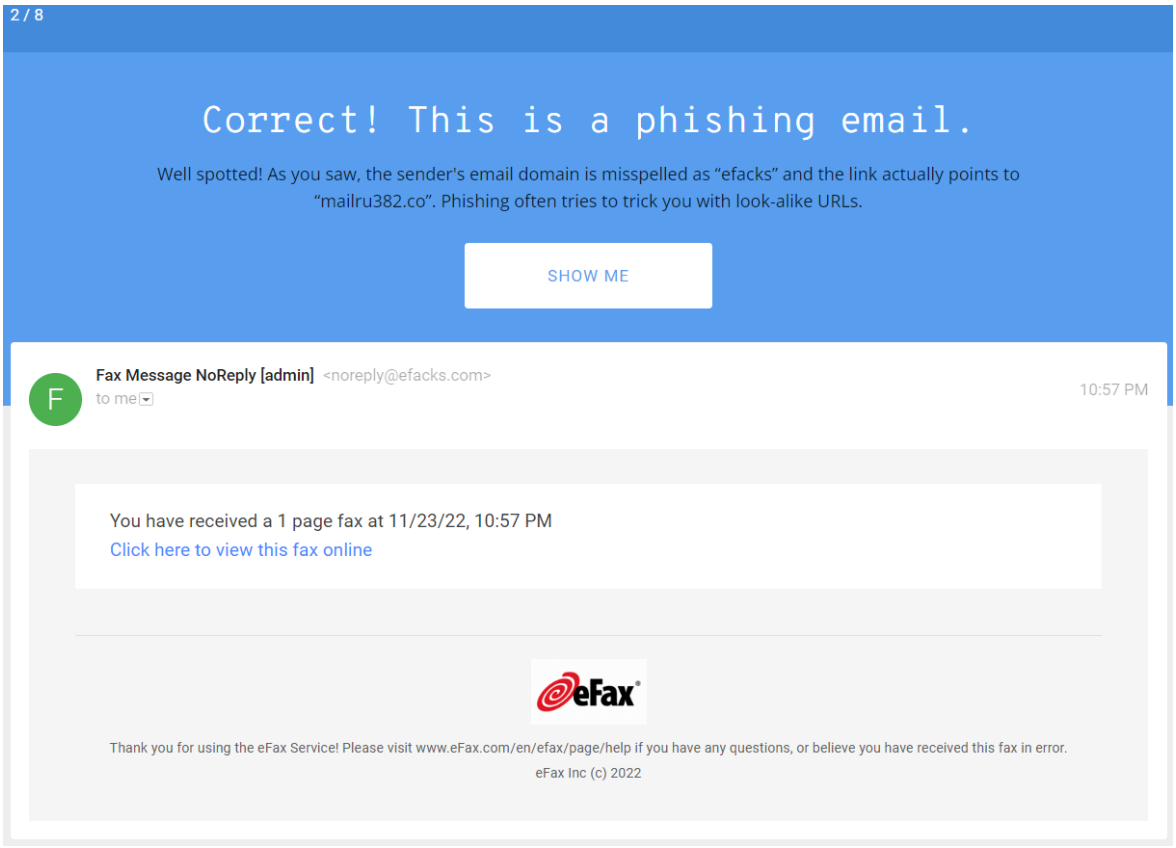
Problem 1:



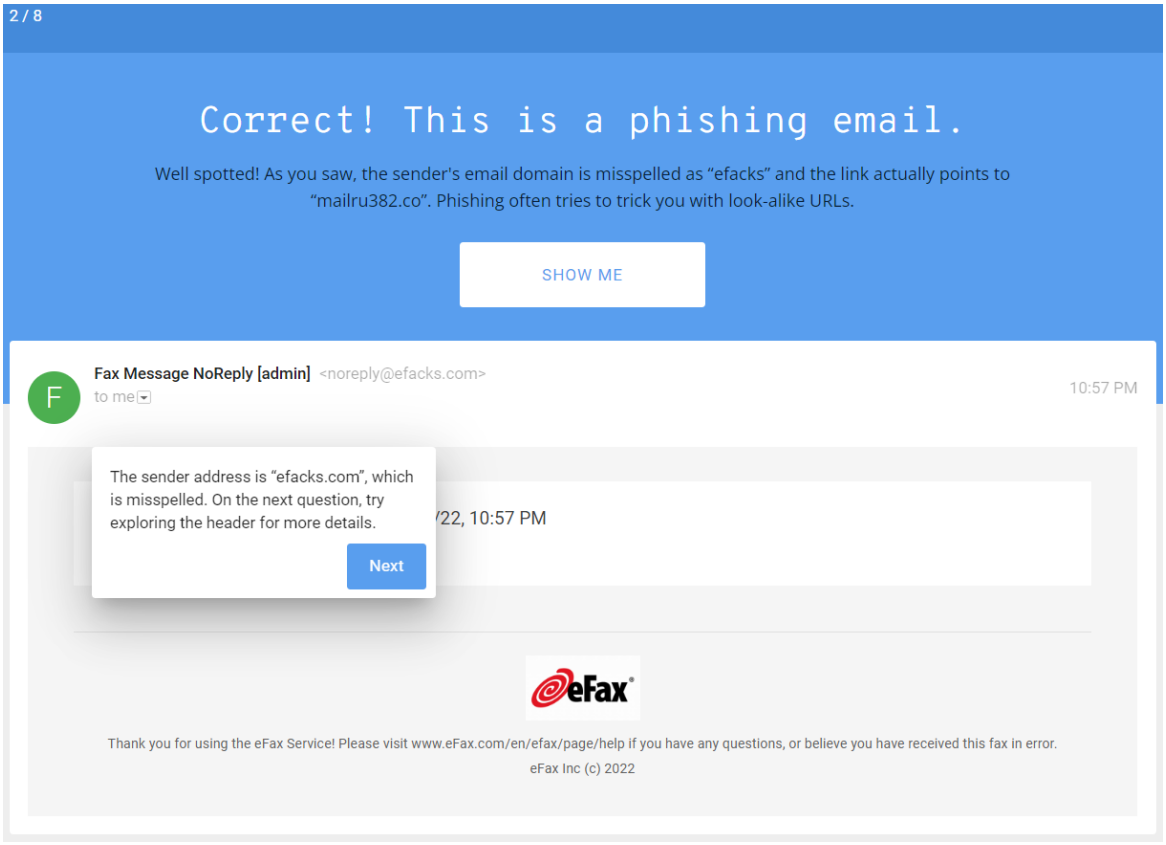
Reason:



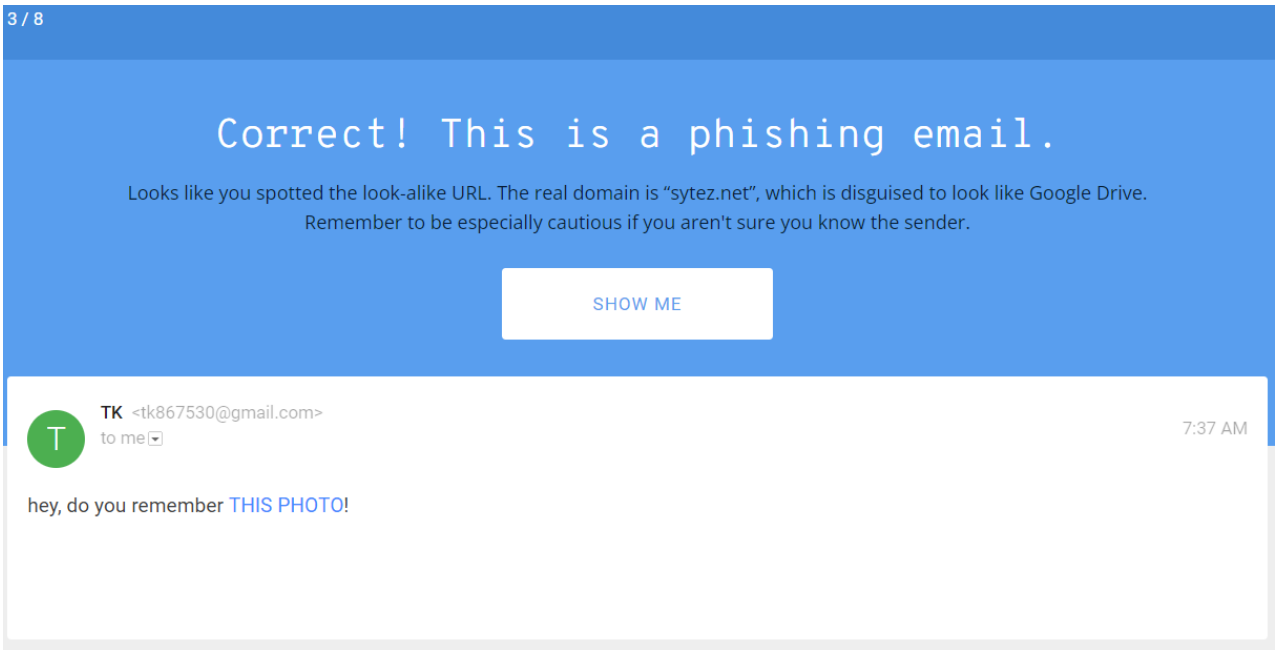
Problem 2:



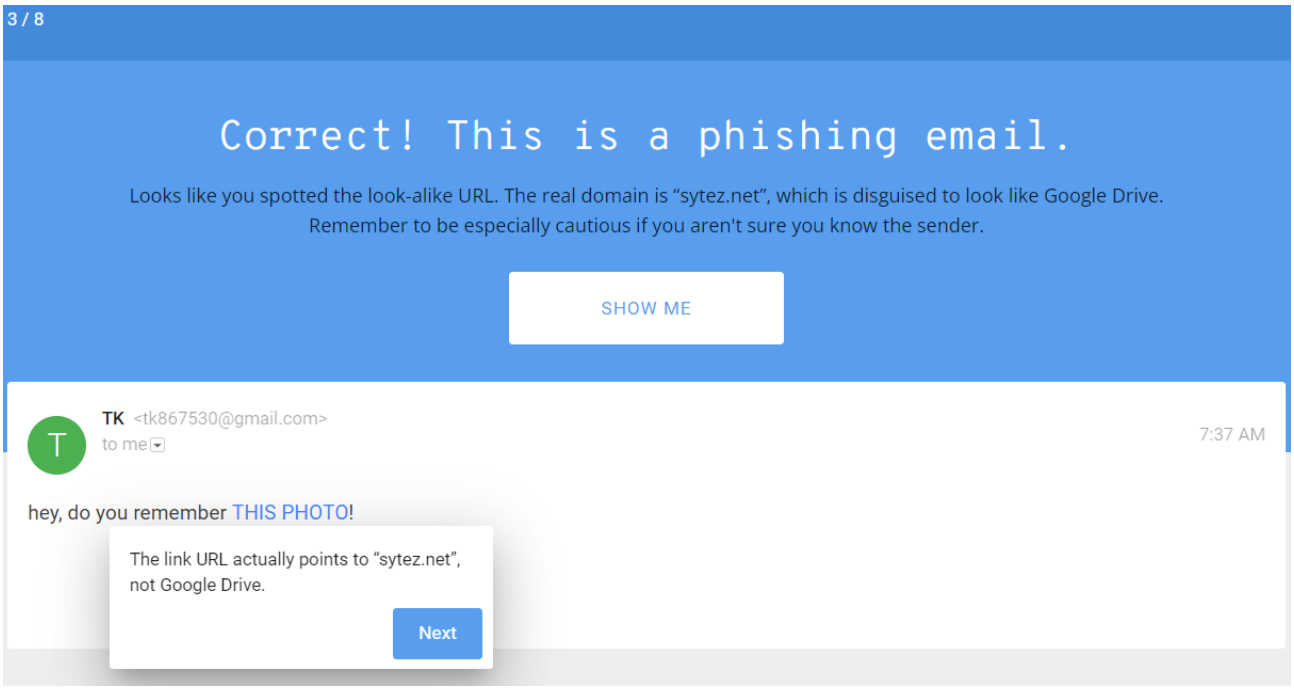
Reason:



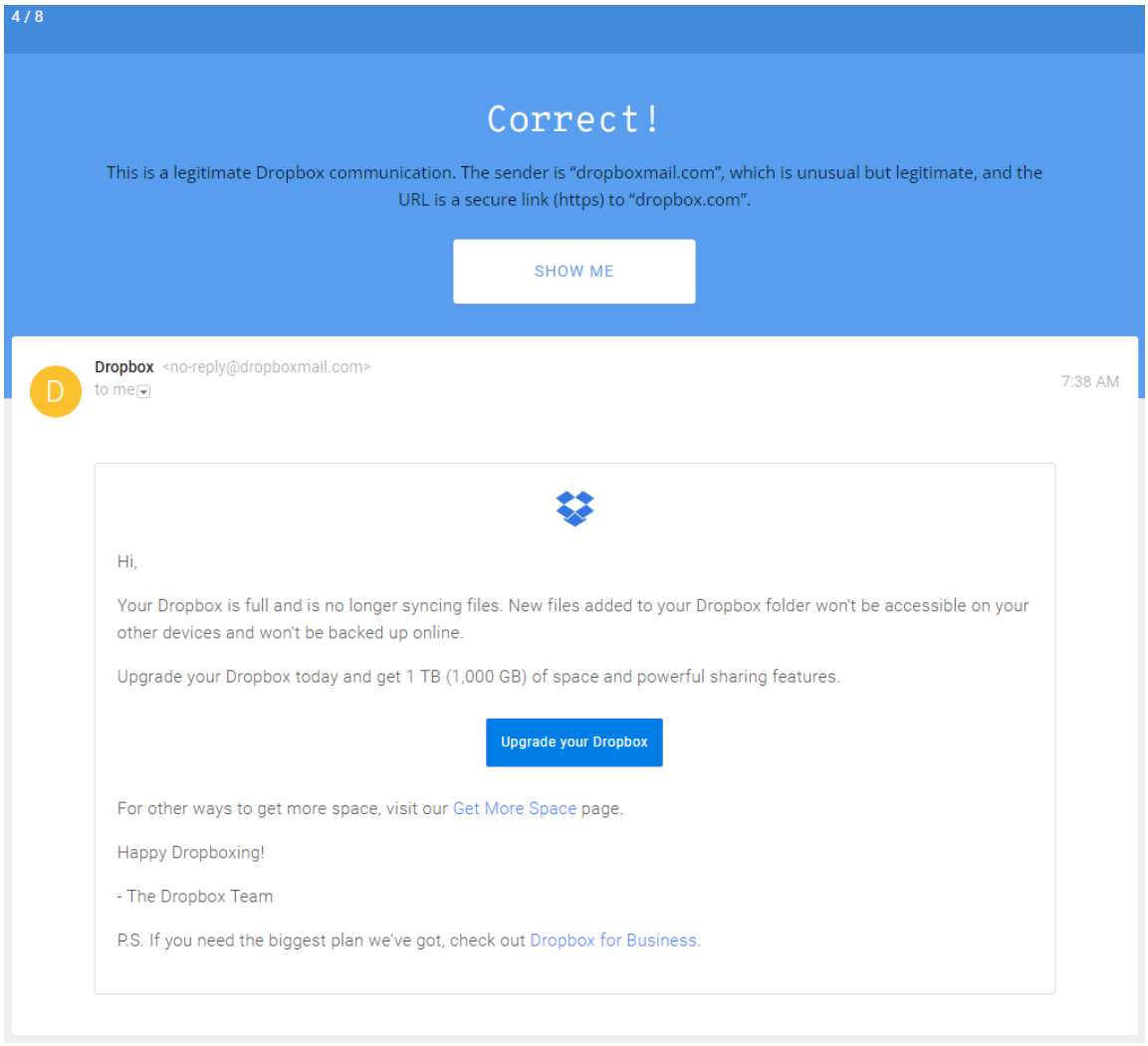
Problem 3:



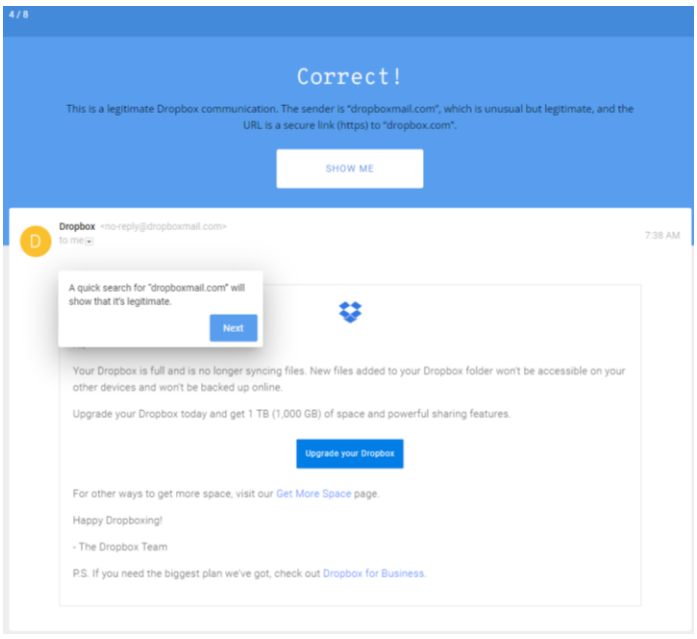
Reason:

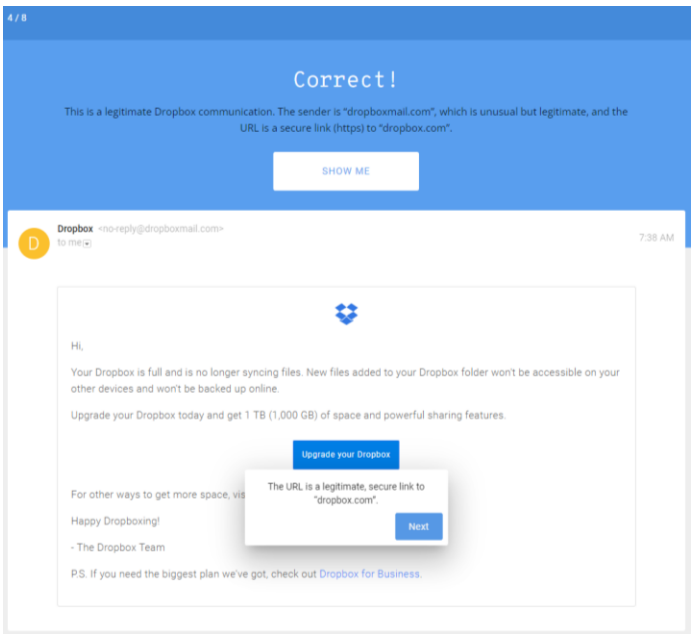


Problem 4:

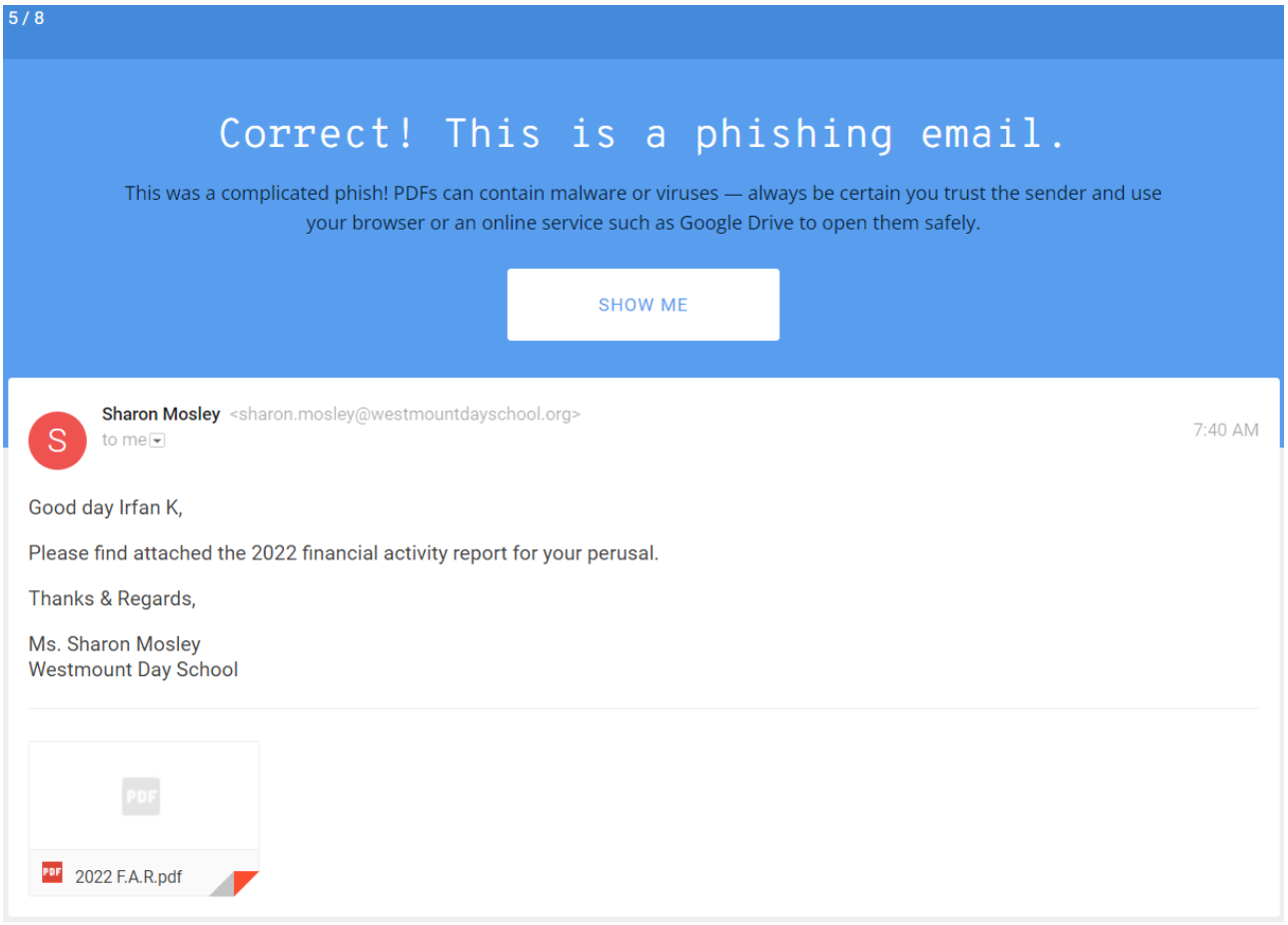


Reason:

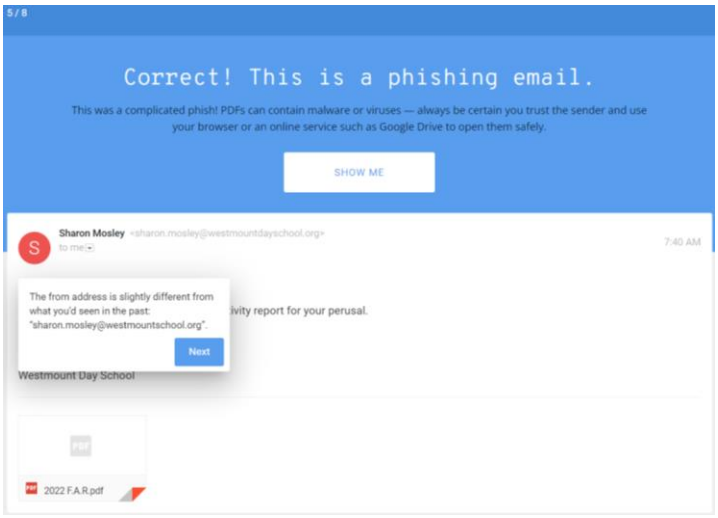


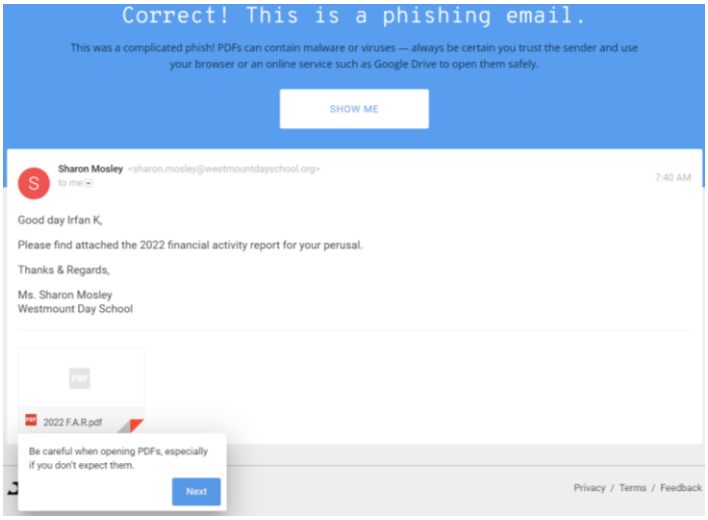


Problem 5:

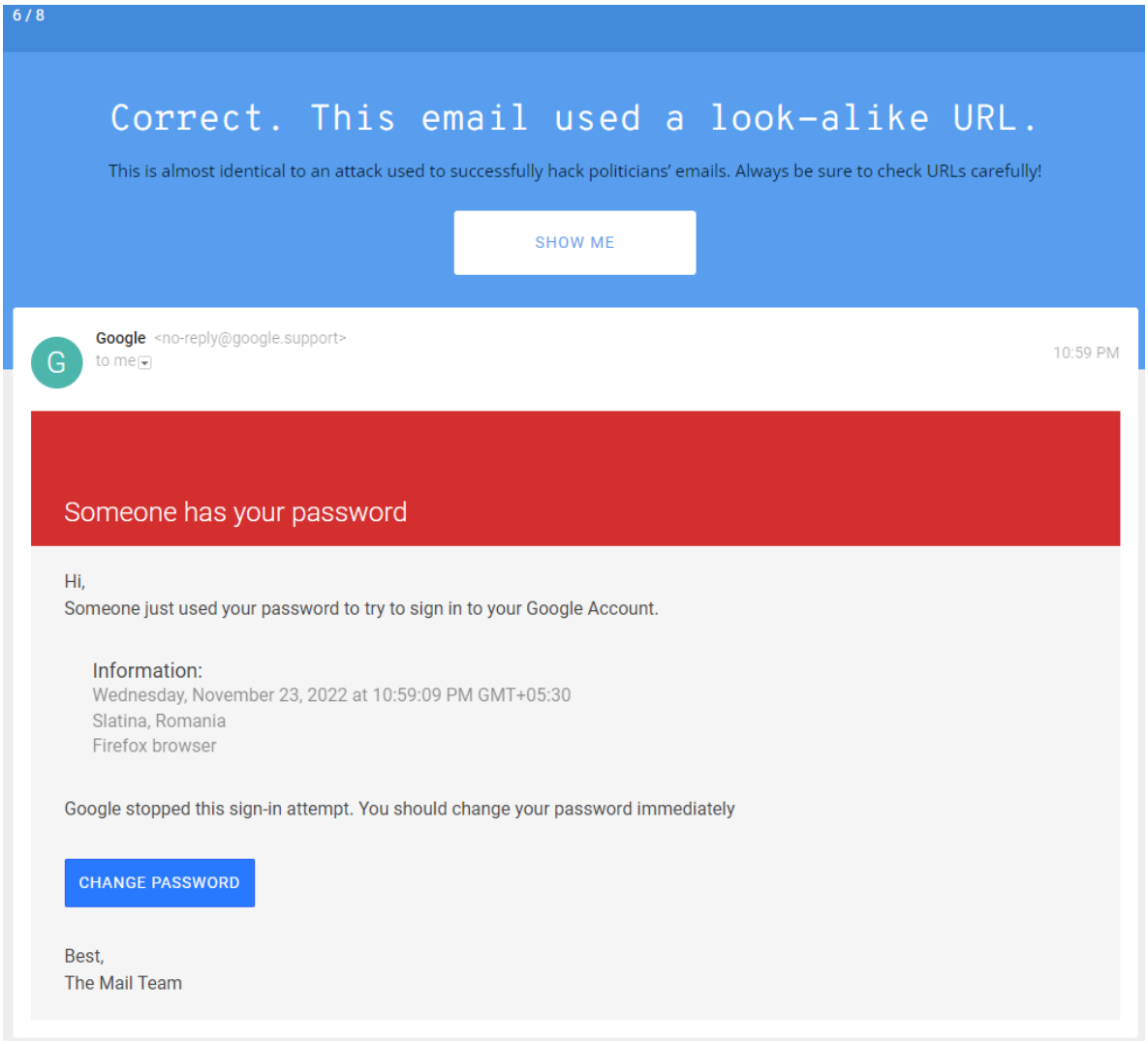


Reason:

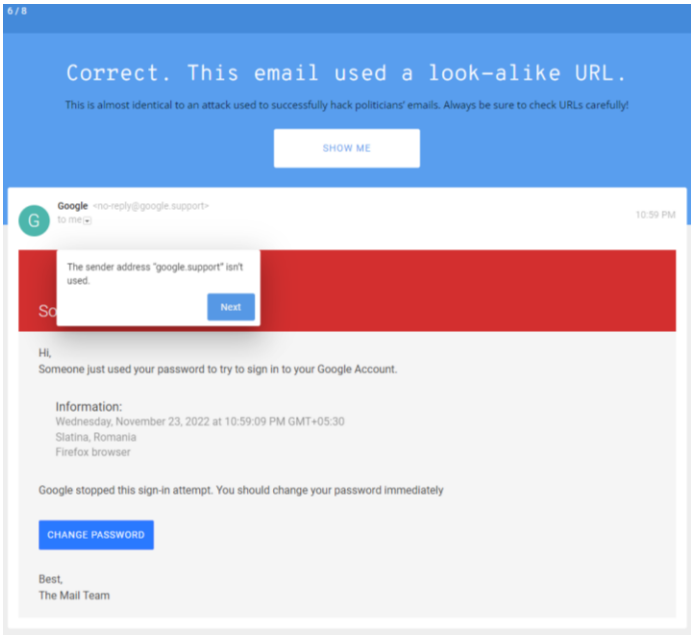


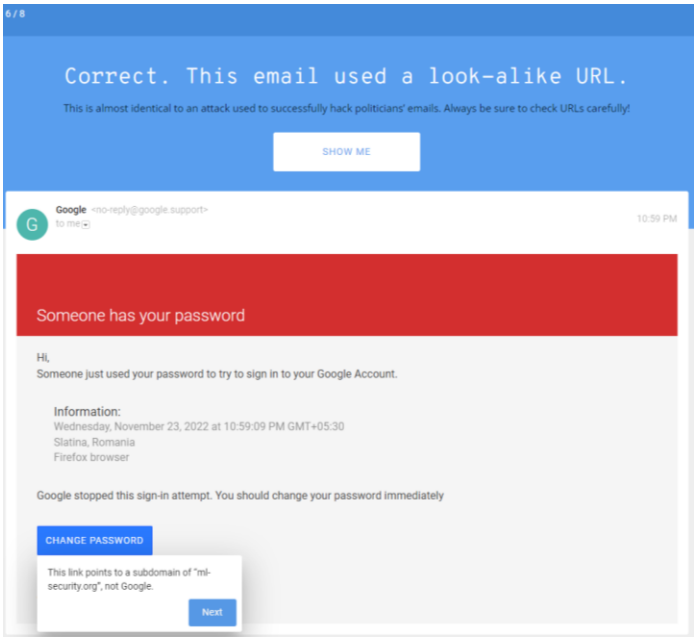


Problem 6:

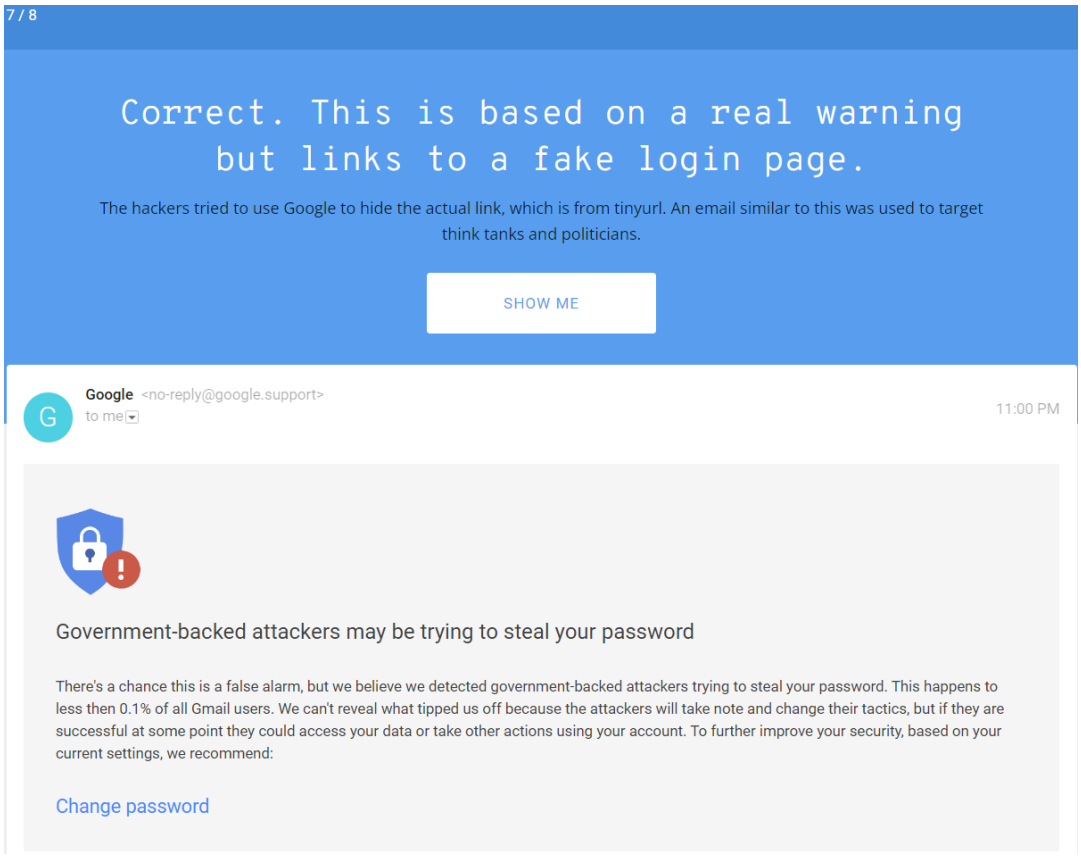


Reason:

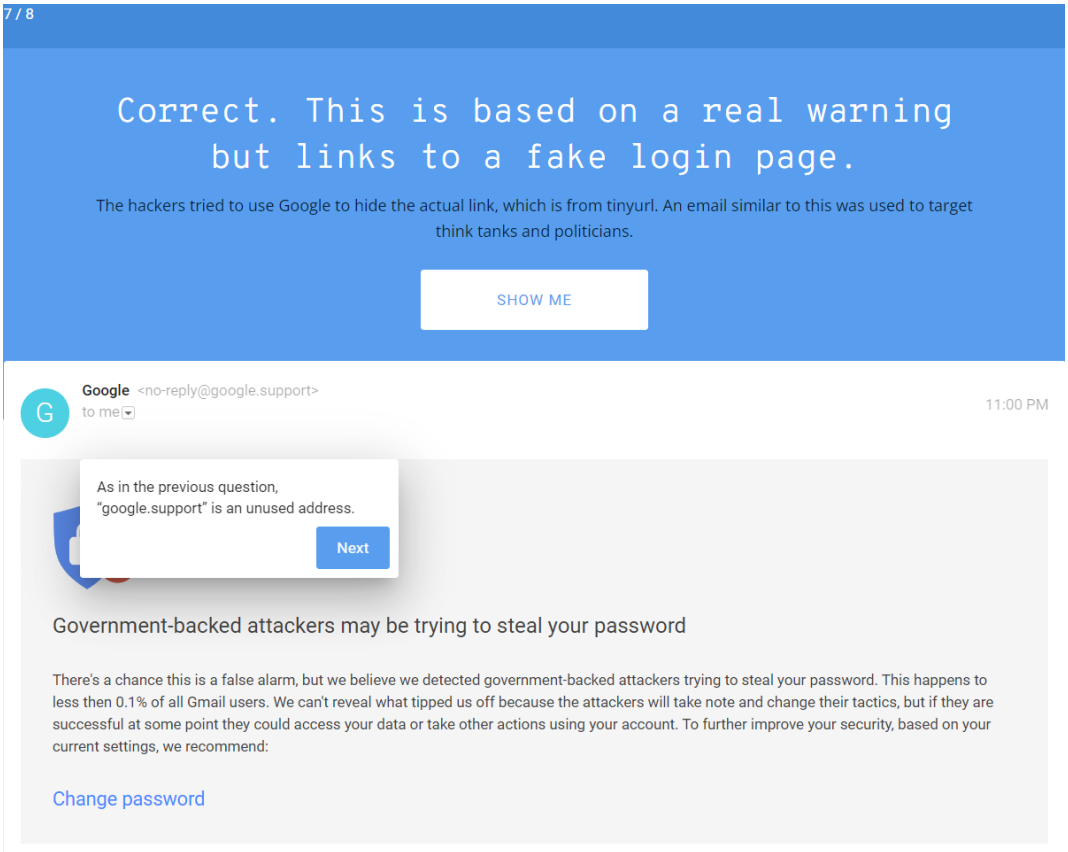




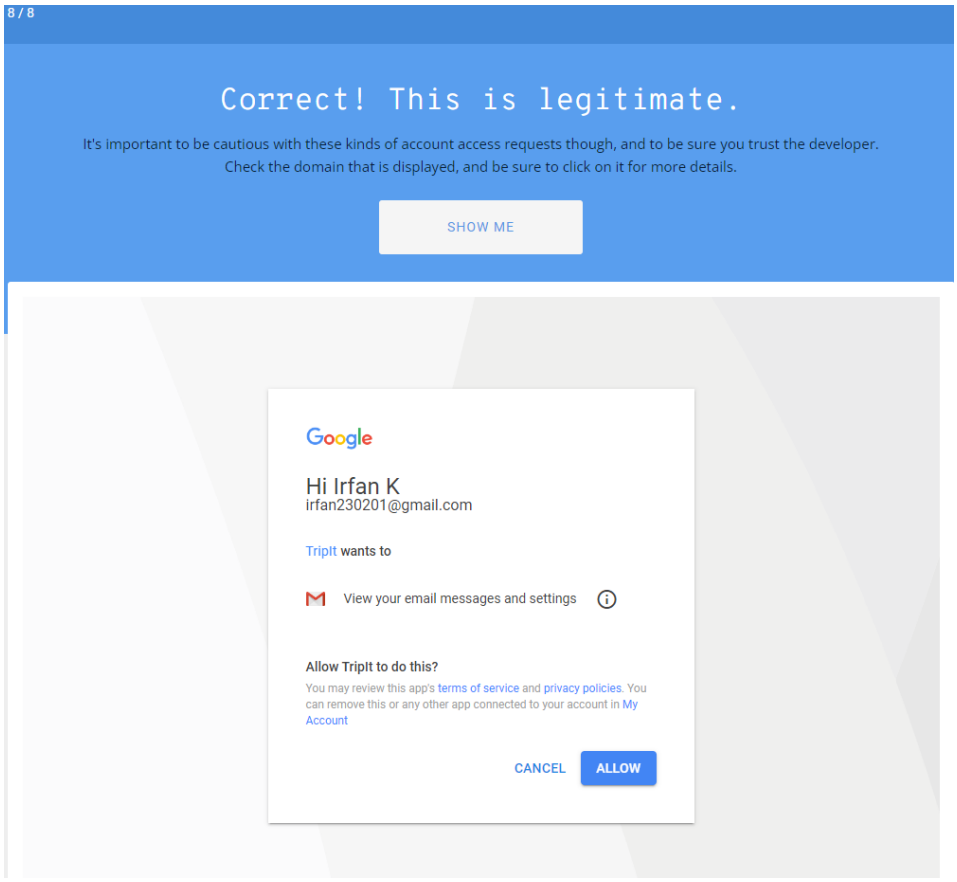
Problem 7:



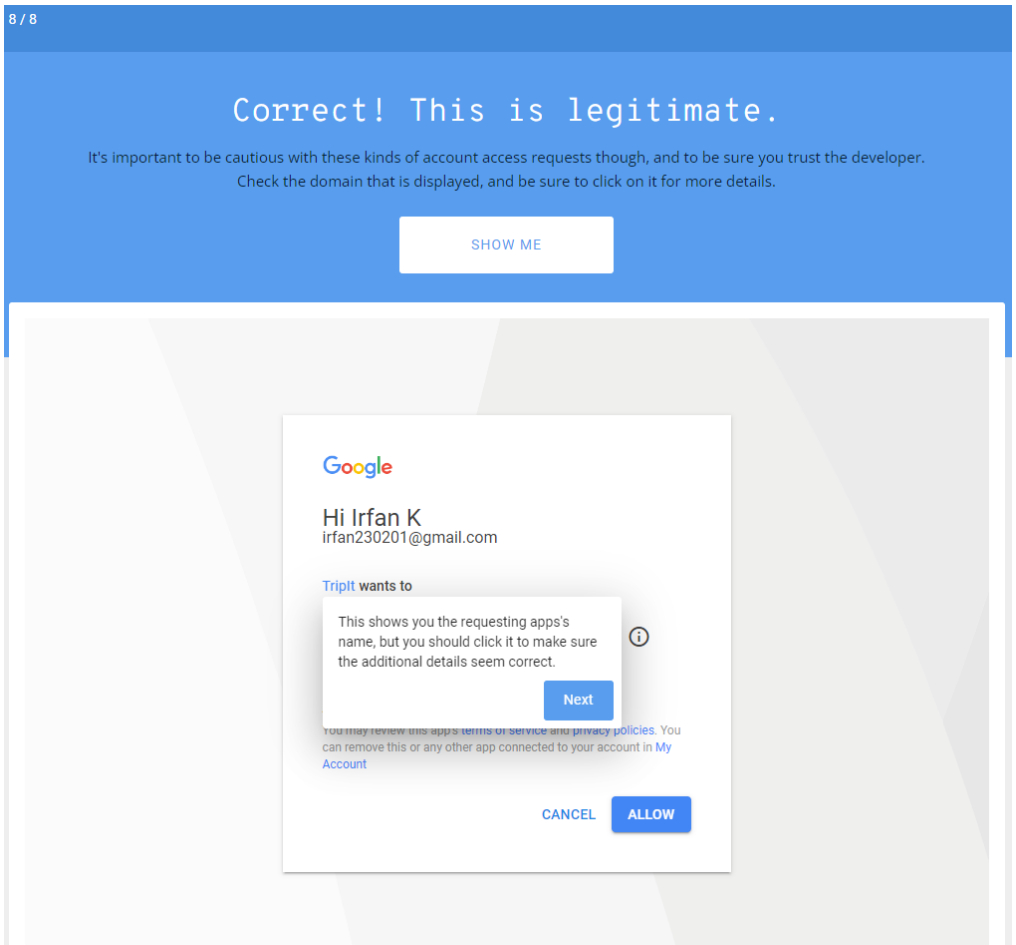
Reason:



Problem 8:



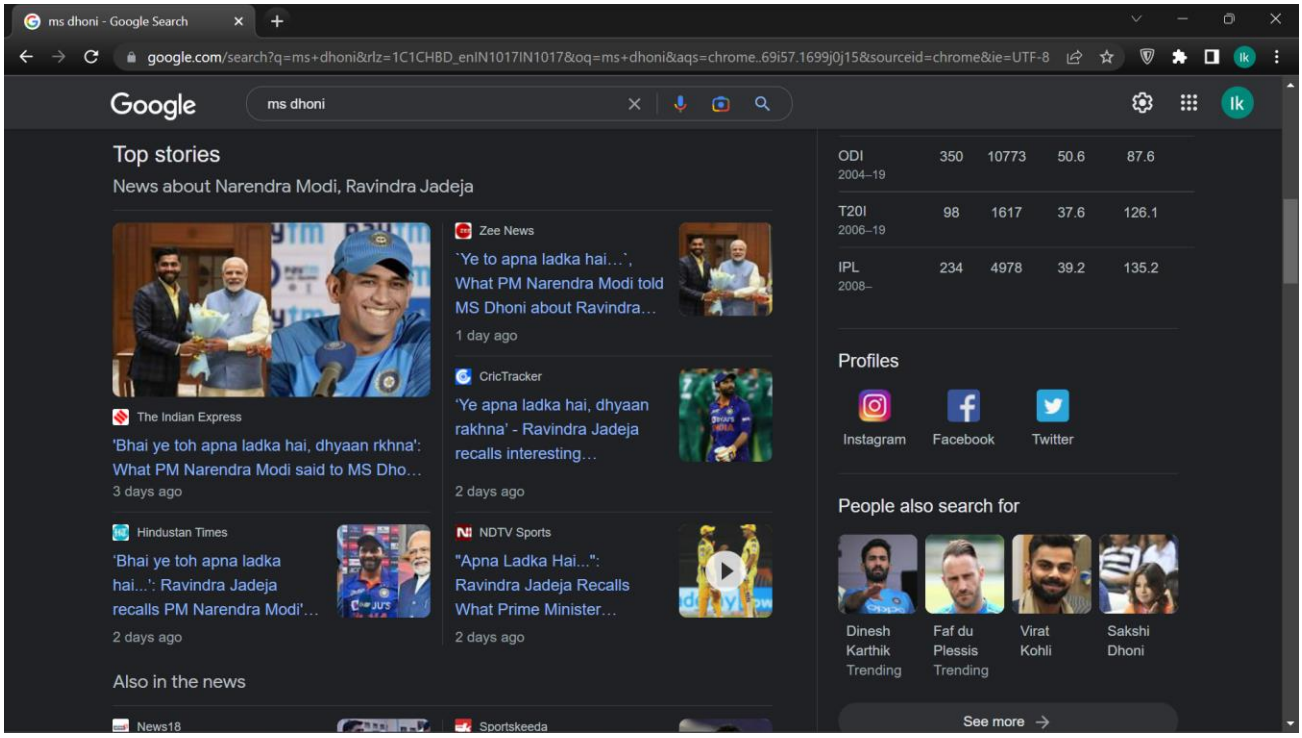
Reason:



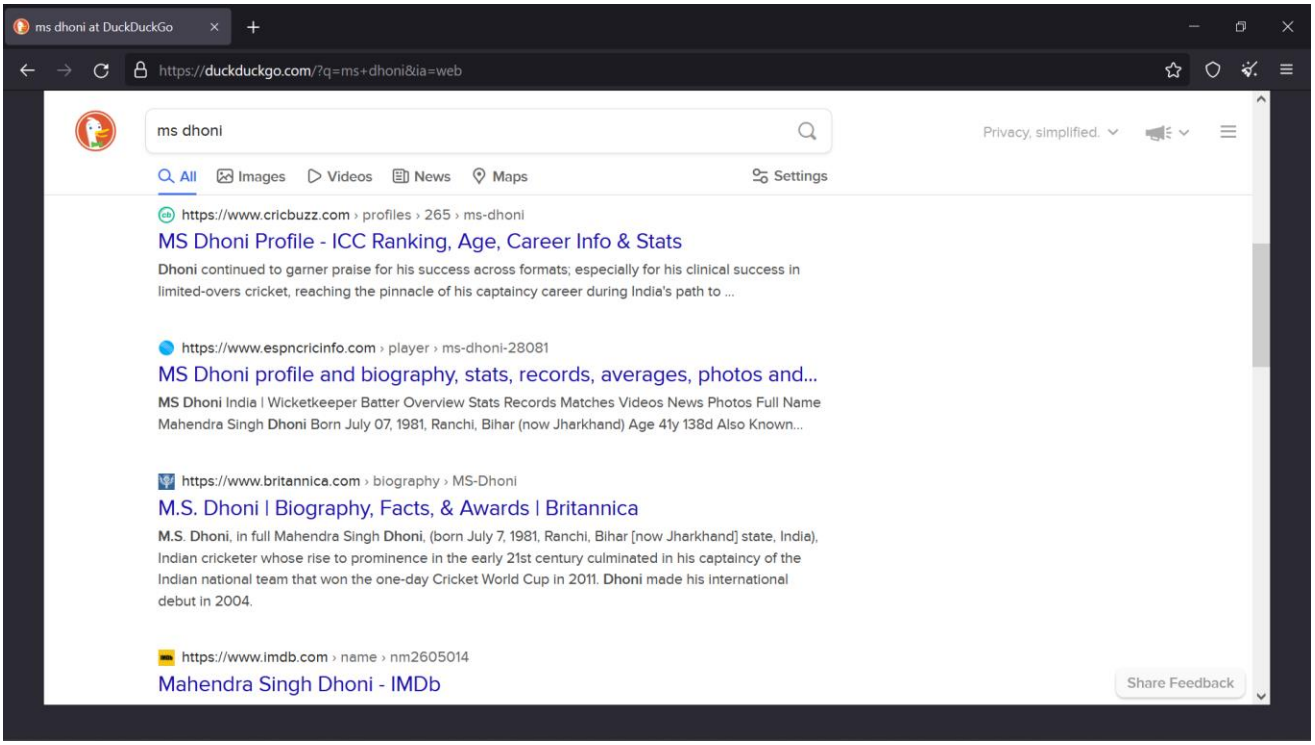
Activity – 2

Task: Compare Chrome search and Torr Browser

Chrome Browser



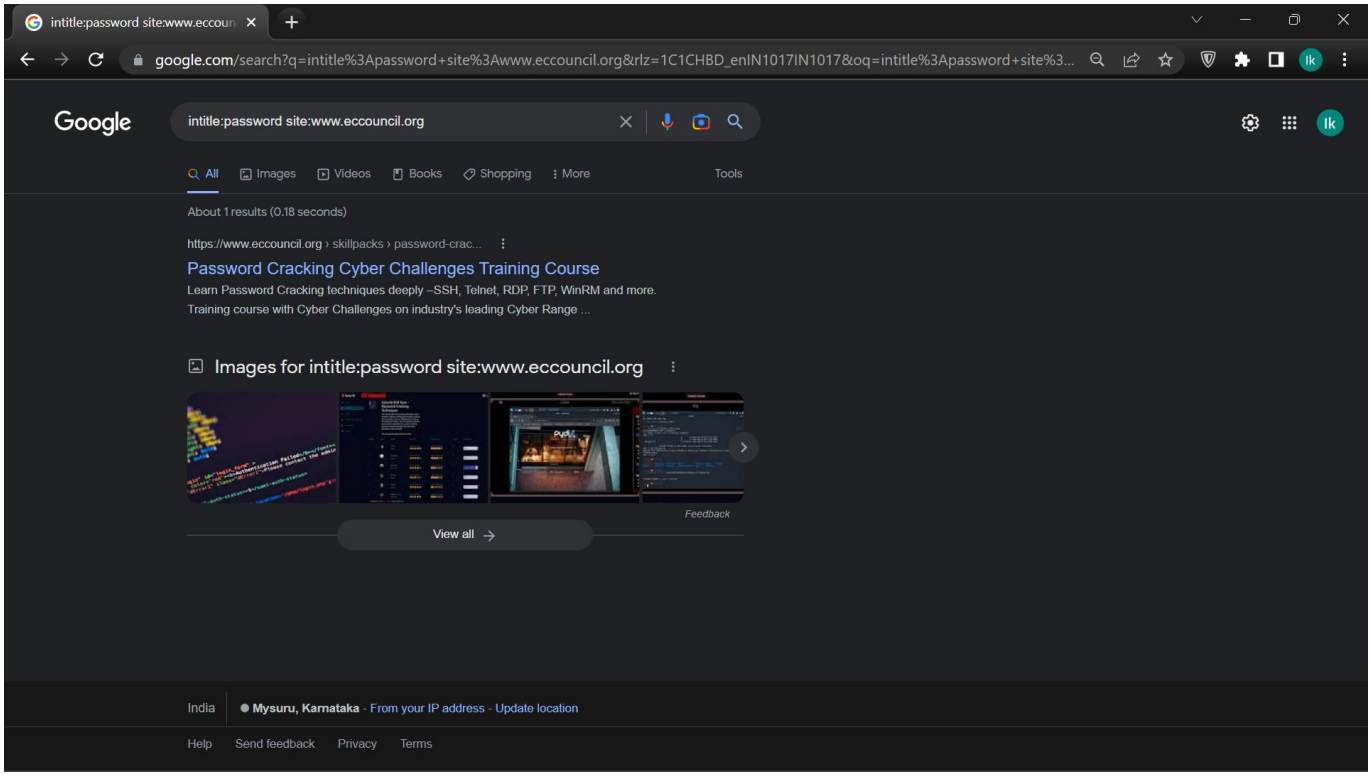
Torr Browser



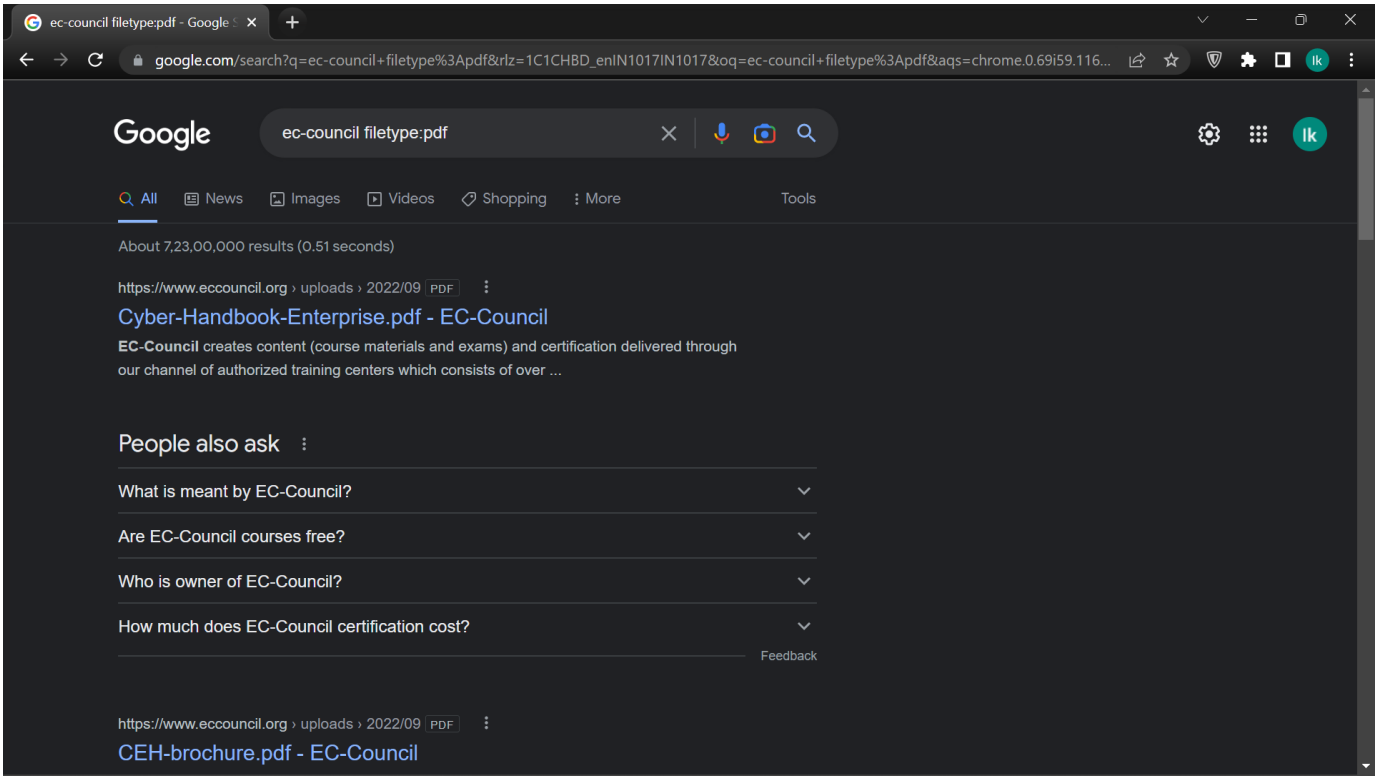
Activity – 3

Google Search Operators

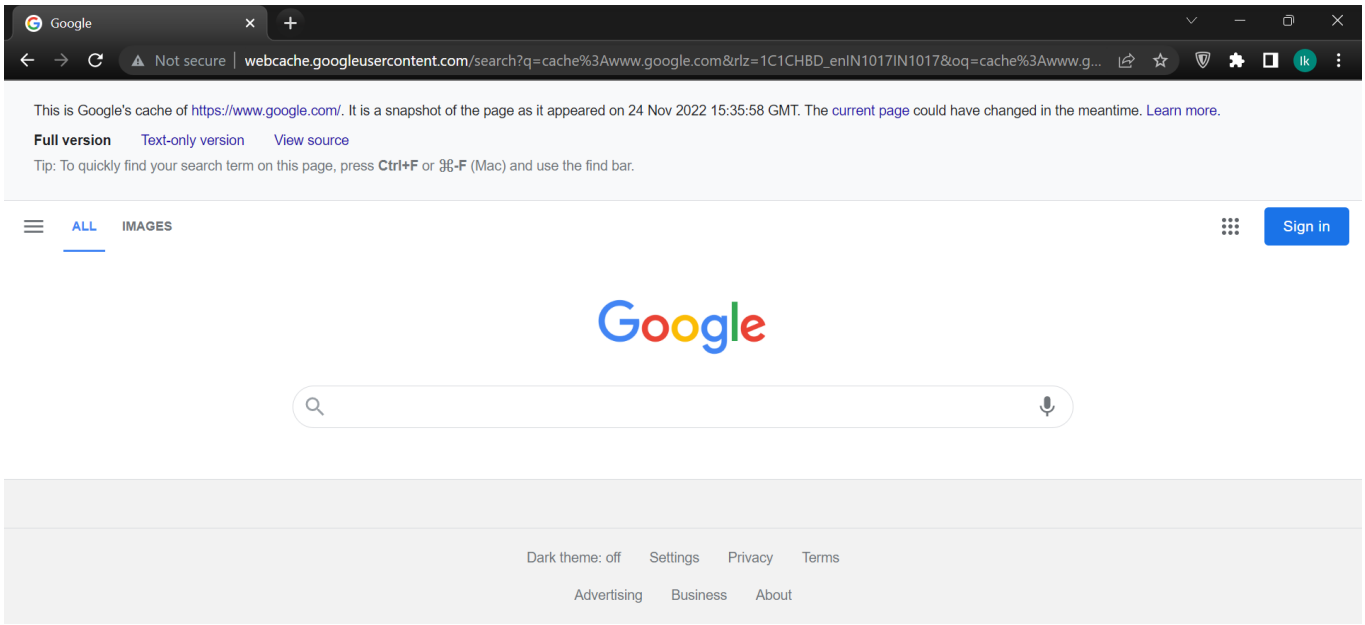
1. intitle



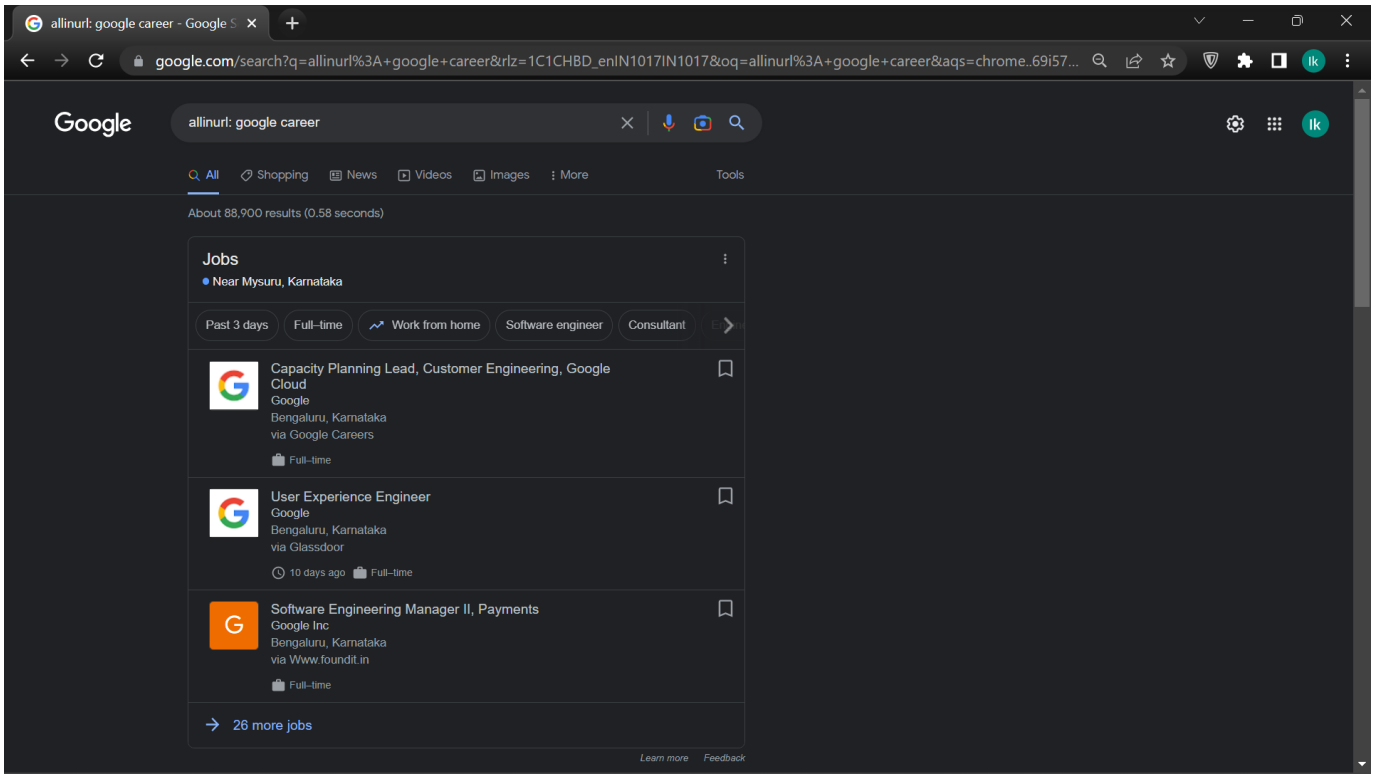
2. filetype



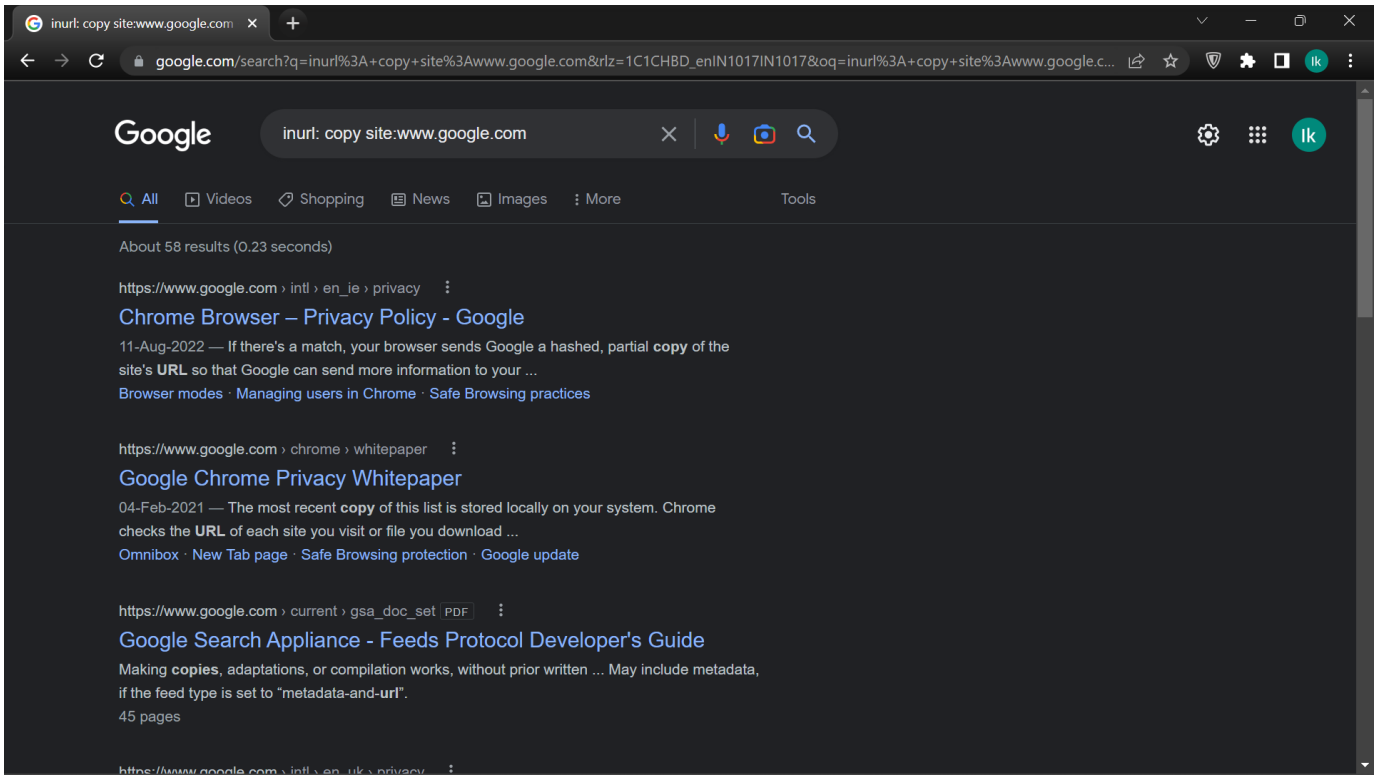
3. cache



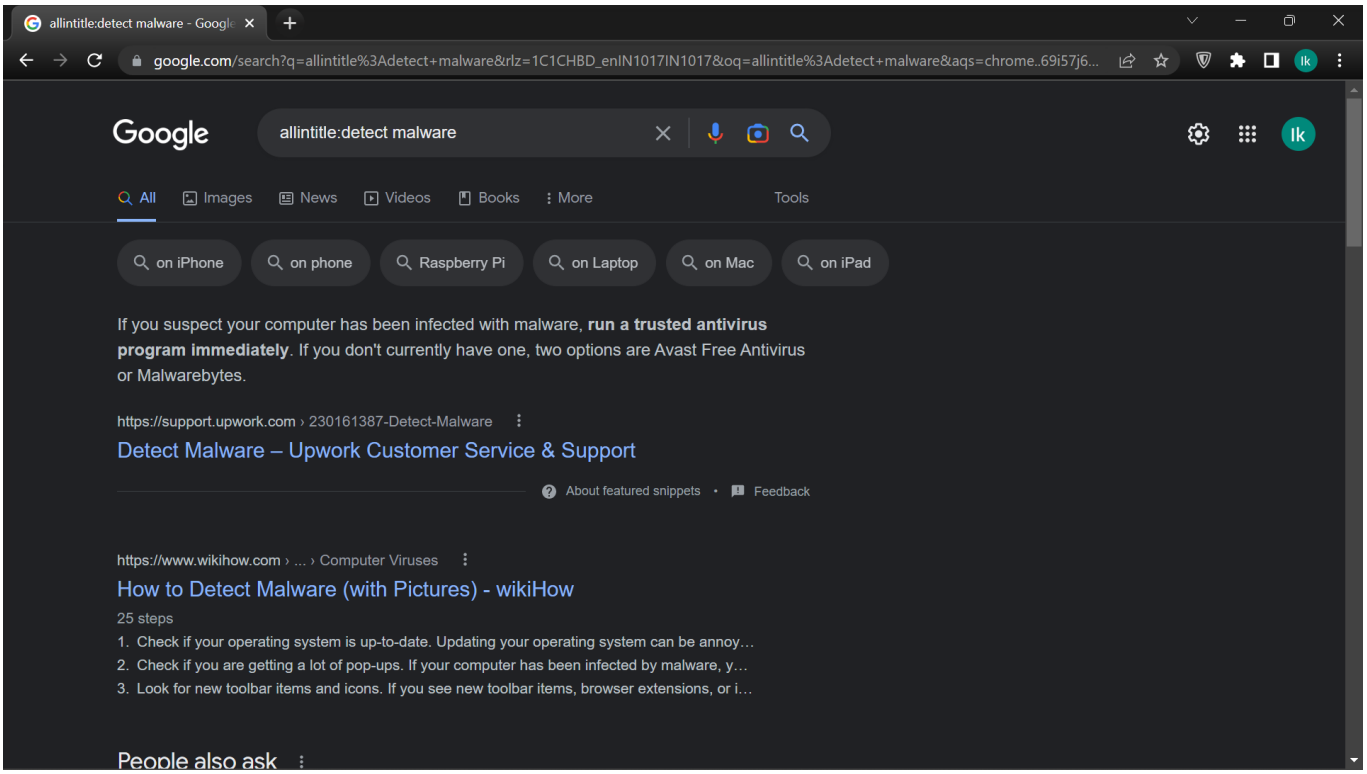
4. allinurl



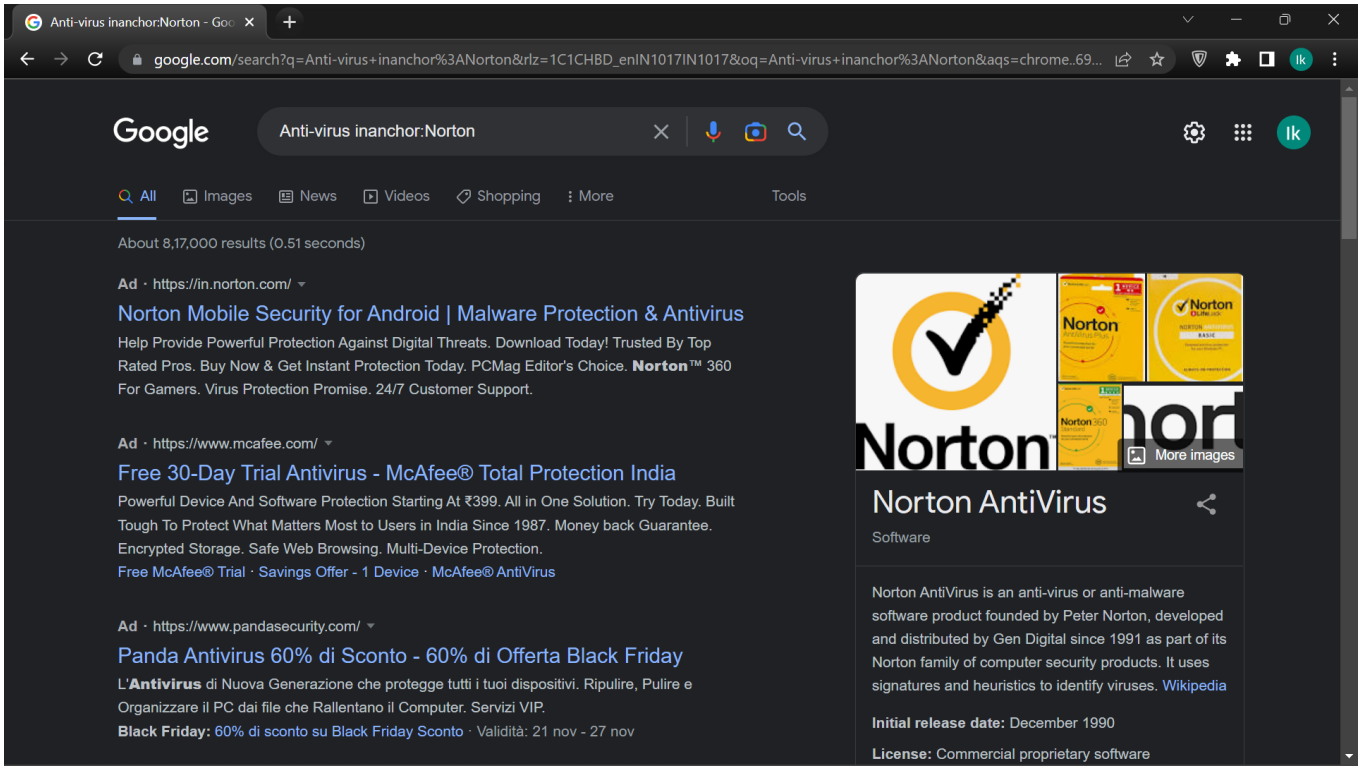
5. inurl



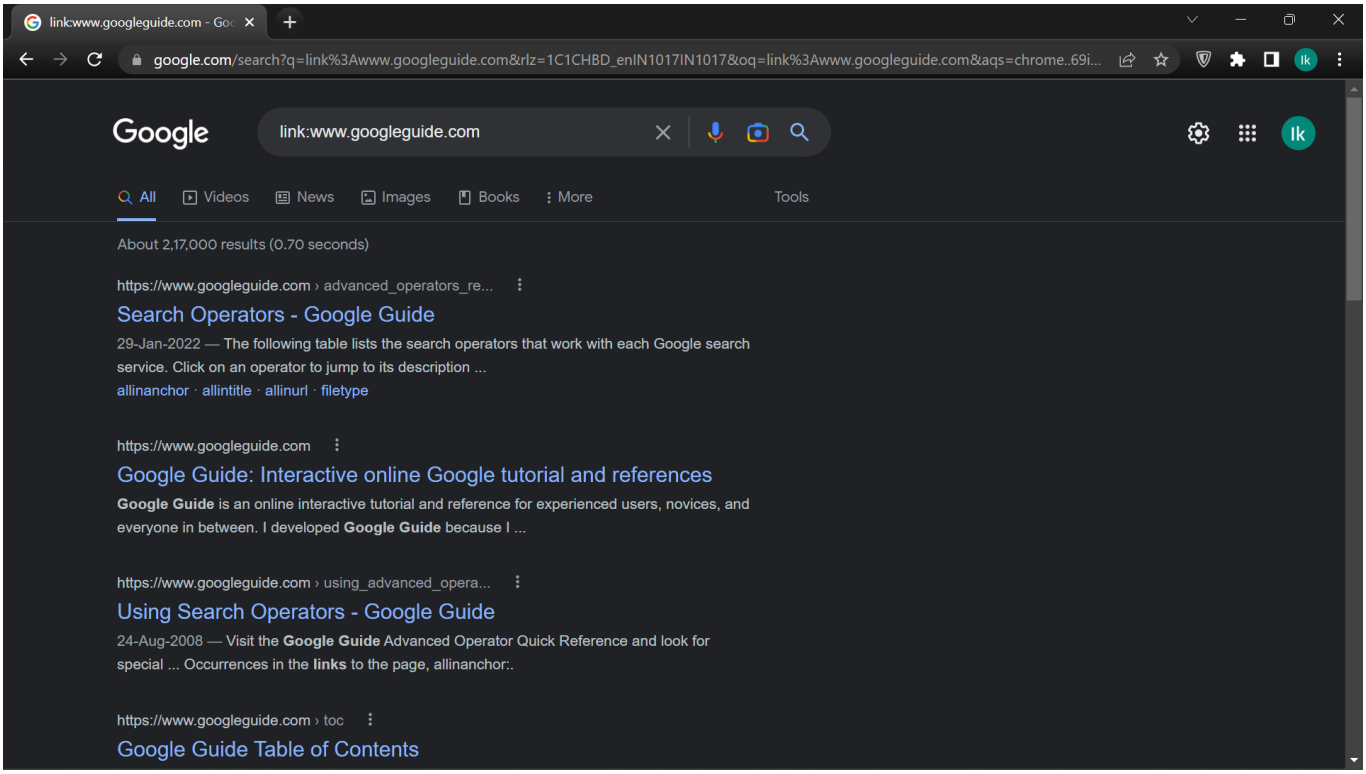
6. allintitle



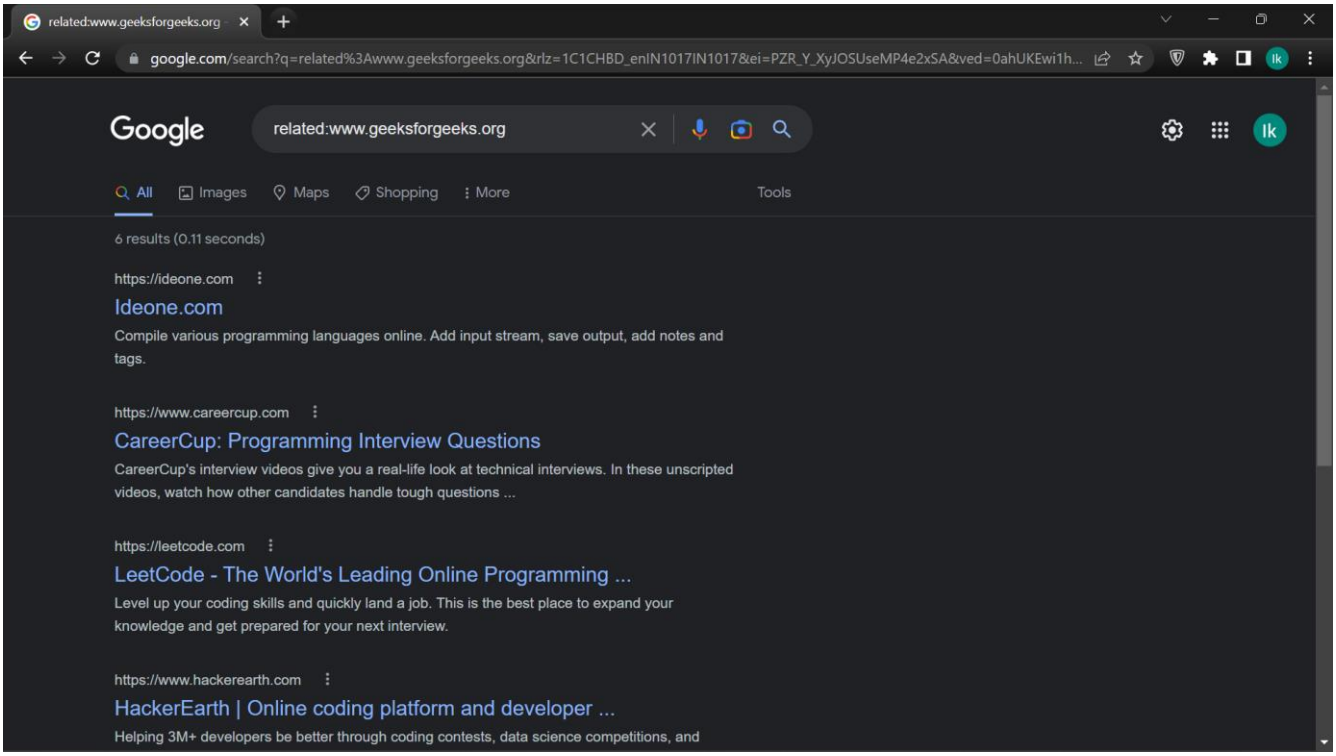
7. inanchor



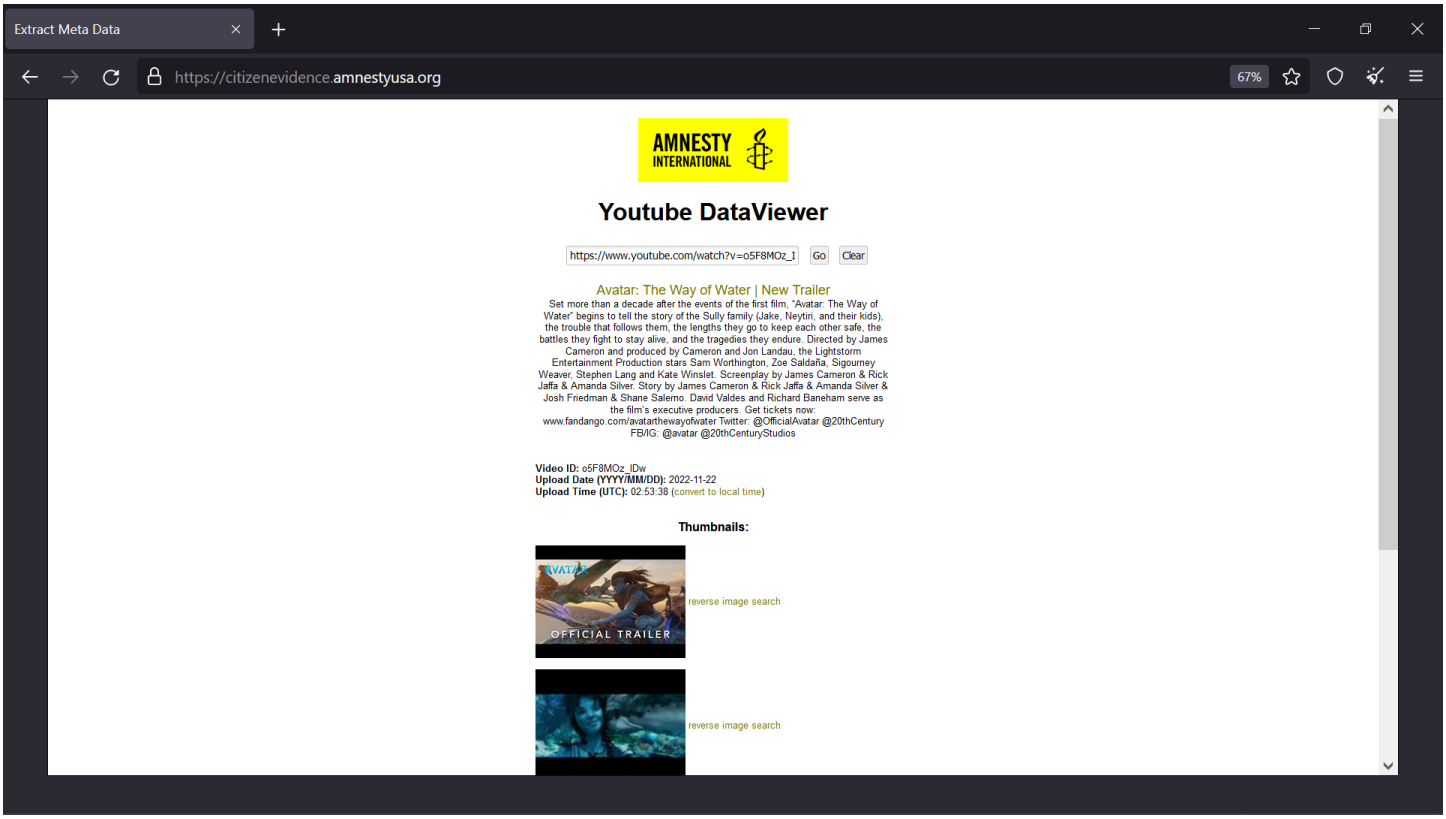
8. link



9. related



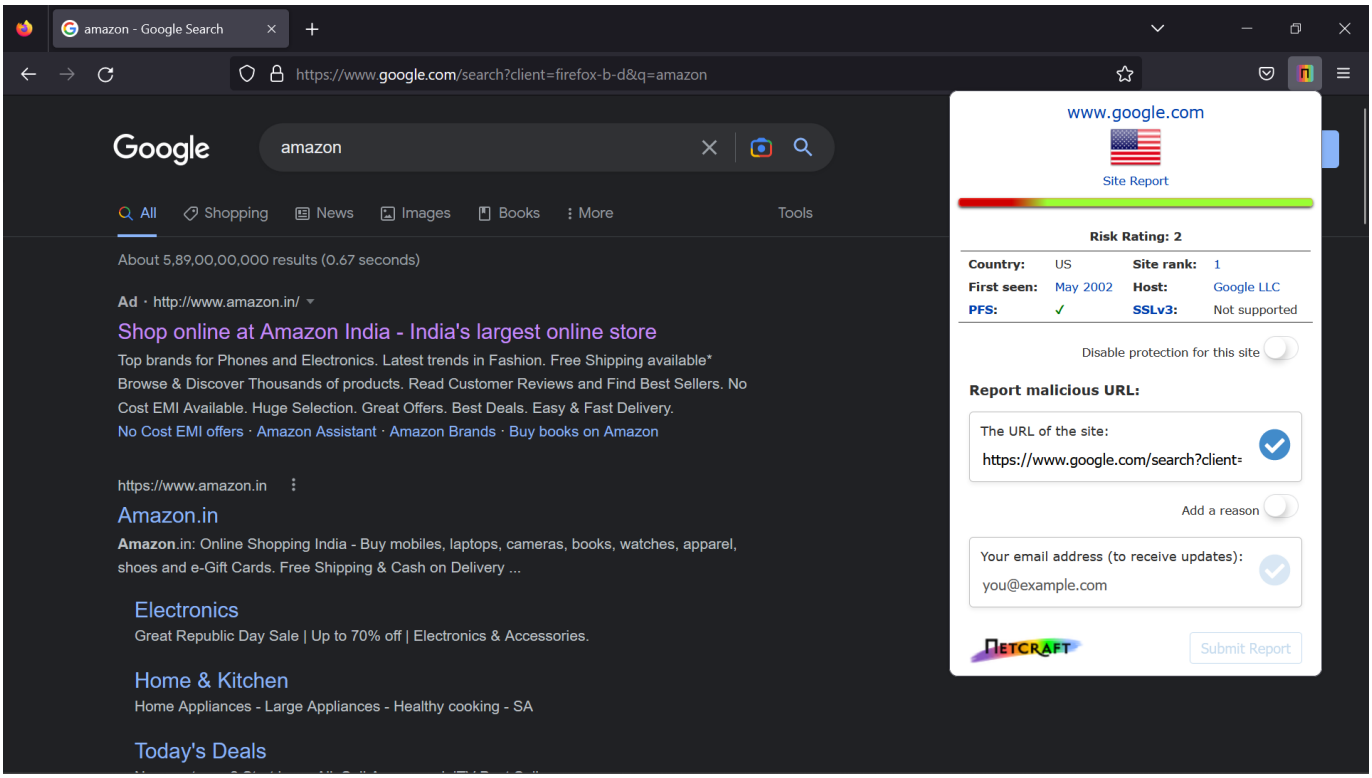
10. Thumbnail Extraction

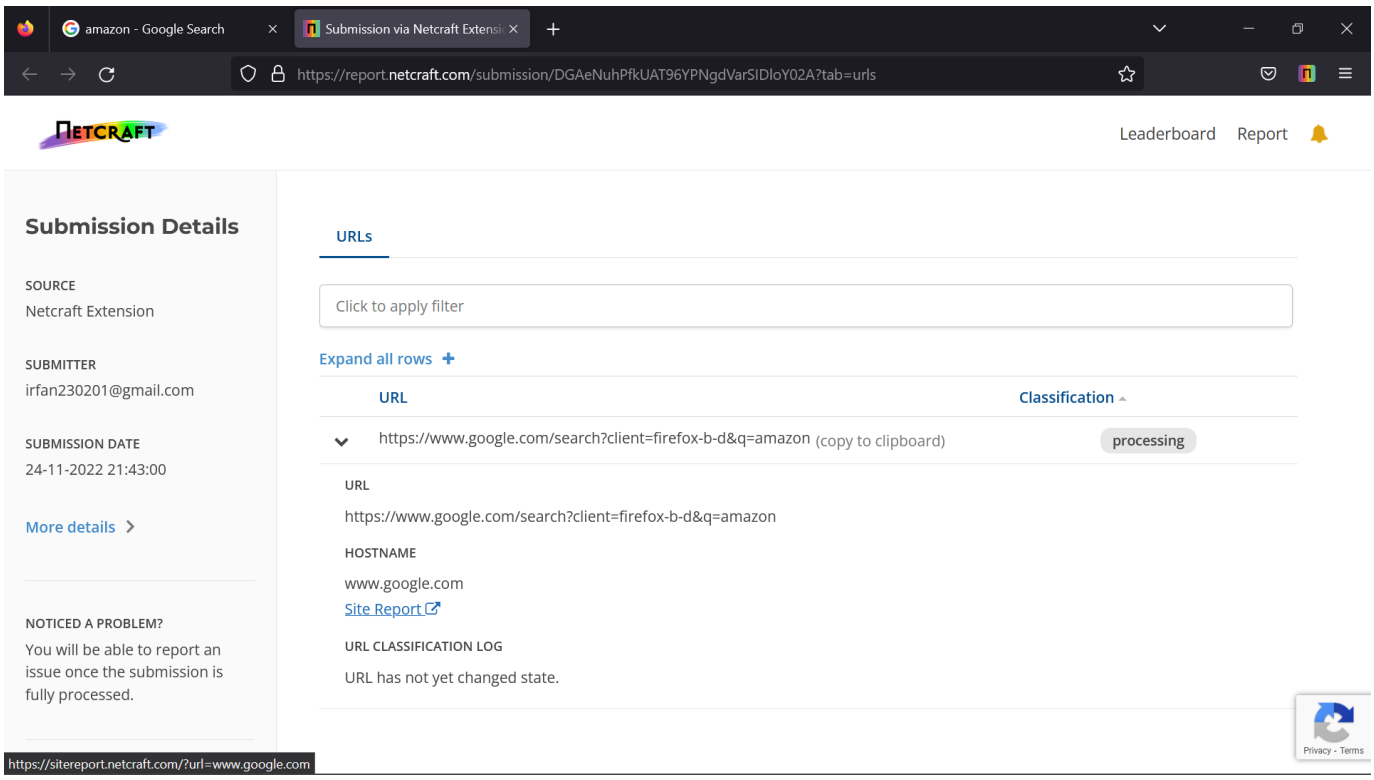


Assignment – 2

Activity - 1

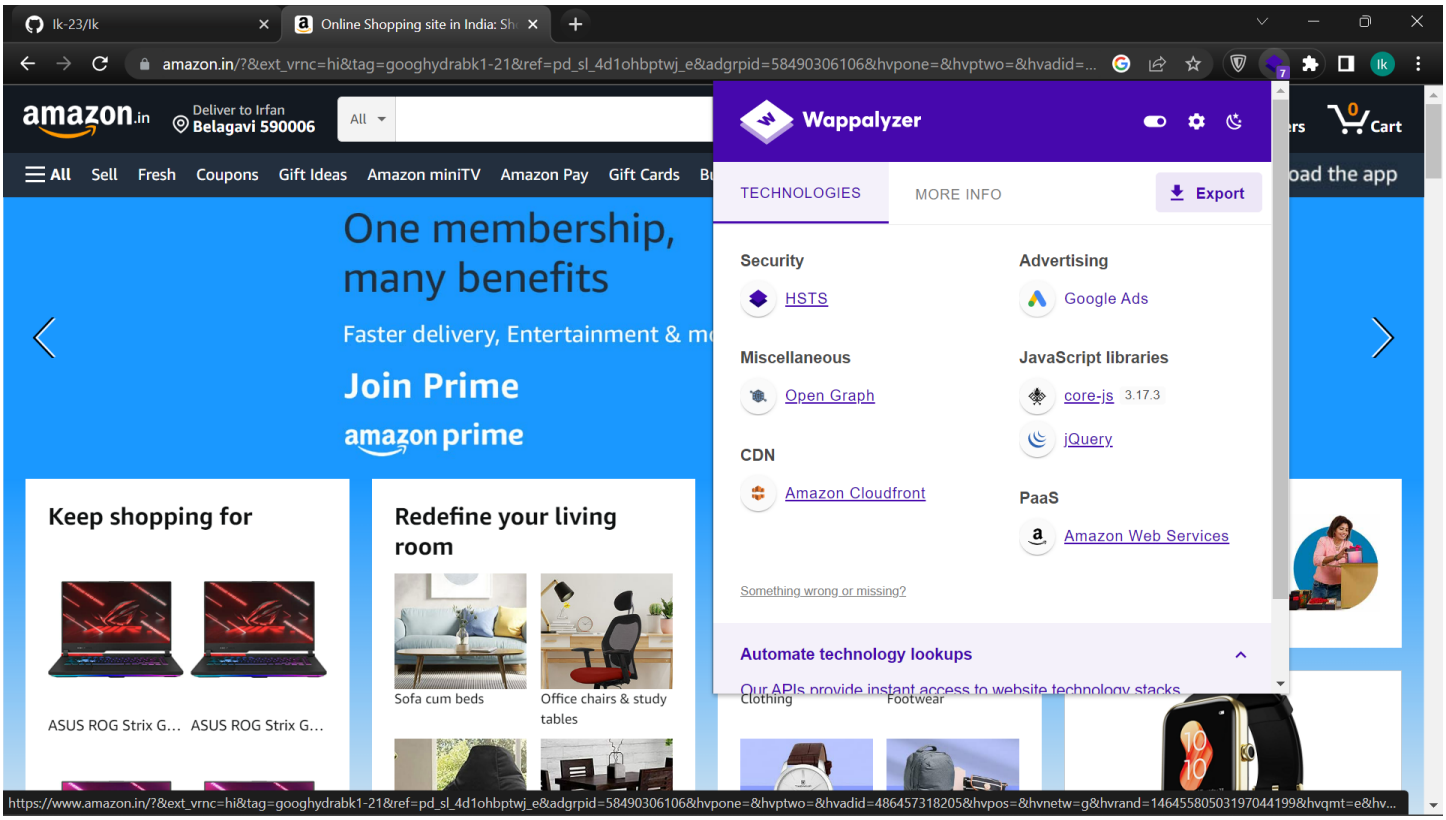
Netcraft: Comprehensive site information and protection from phishing and malicious JavaScript when browsing the web.





Activity - 2

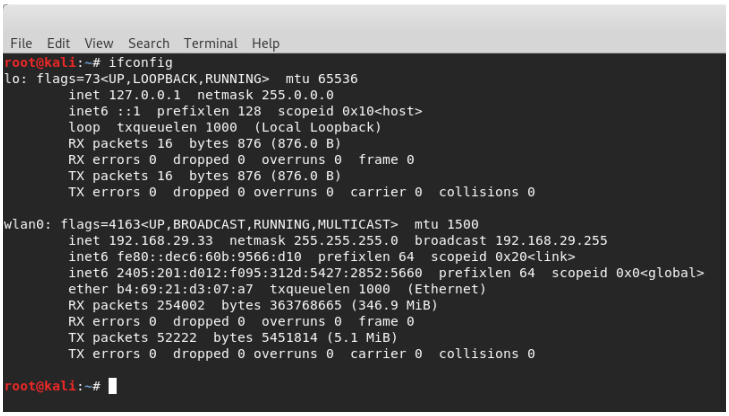
Wappalyzer



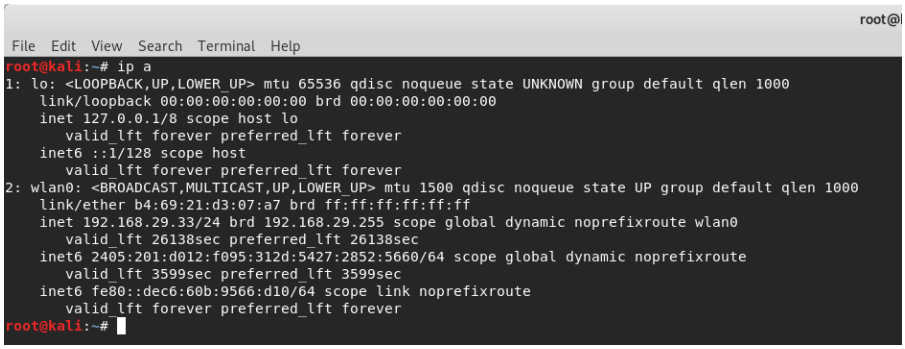
Activity – 3

Kali-Linux commands

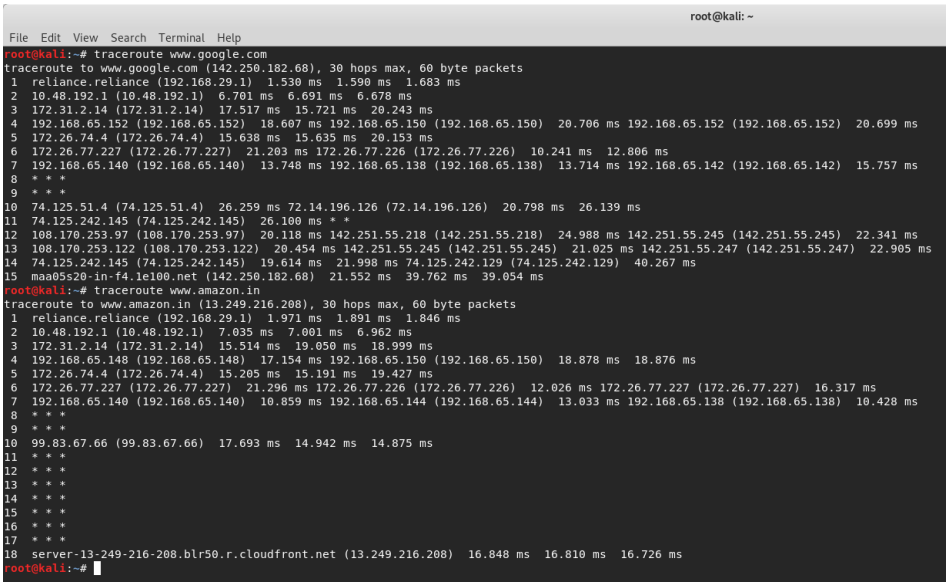
1. ifconfig



2. ip



3. traceroute



4. netstat

```
File  Edit  View  Search  Terminal  Help
root@kali:~# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    34828    /run/user/0/systemd/notify
unix  3      [ ]         DGRAM                    14121    /run/systemd/notify
unix  2      [ ]         DGRAM                    29509    /run/wpa_supplicant/wlan0
unix  6      [ ]         DGRAM                    14160    /run/systemd/journal/socket
unix  12     [ ]         DGRAM                    14170    /run/systemd/journal/dev-log
unix  2      [ ]         DGRAM                    14213    /run/systemd/journal/syslog
unix  2      [ ]         DGRAM                    33943    /run/wpa_supplicant/p2p-dev-wlan0
unix  2      [ ]         DGRAM                    43590
unix  3      [ ]         STREAM     CONNECTED     35634    /run/user/0/bus
unix  3      [ ]         STREAM     CONNECTED     28350
unix  3      [ ]         STREAM     CONNECTED     38306
unix  3      [ ]         STREAM     CONNECTED     28625    @/tmp/.ICE-unix/1149
unix  3      [ ]         STREAM     CONNECTED     38275    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     34049    /run/user/0/bus
unix  3      [ ]         STREAM     CONNECTED     27384
unix  3      [ ]         STREAM     CONNECTED     37626
unix  3      [ ]         STREAM     CONNECTED     40100    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     36183    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     38235    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     28505
unix  3      [ ]         STREAM     CONNECTED     36393    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     37474    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     32504    /run/user/0/bus
unix  3      [ ]         STREAM     CONNECTED     43344    /run/user/0/bus
unix  3      [ ]         STREAM     CONNECTED     43022
unix  3      [ ]         STREAM     CONNECTED     30340
unix  3      [ ]         STREAM     CONNECTED     43299
```

5. dig

```
File  Edit  View  Search  Terminal  Help
root@kali:~# dig google.com

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8786
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             252     IN      A       142.250.195.46

;; Query time: 16 msec
;; SERVER: 192.168.29.1#53(192.168.29.1)
;; WHEN: Wed Nov 23 23:16:35 UTC 2022
;; MSG SIZE  rcvd: 55

root@kali:~#
```

6. nslookup

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nslookup amazon.com
Server:         192.168.29.1
Address:        192.168.29.1#53

Non-authoritative answer:
Name:   amazon.com
Address: 205.251.242.103
Name:   amazon.com
Address: 54.239.28.85
Name:   amazon.com
Address: 52.94.236.248

root@kali:~# nslookup google.com
Server:         192.168.29.1
Address:        192.168.29.1#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.195.46
Name:   google.com
Address: 2404:6800:4007:822::200e

root@kali:~#
```

7. route

```
File  Edit  View  Search  Terminal  Help
root@kali:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         reliance.relian 0.0.0.0         UG    600    0        0 wlan0
192.168.29.0    0.0.0.0         255.255.255.0   U     600    0        0 wlan0
root@kali:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.29.1    0.0.0.0         UG    600    0        0 wlan0
192.168.29.0    0.0.0.0         255.255.255.0   U     600    0        0 wlan0
root@kali:~# route -Cn
Kernel IP routing cache
Source          Destination     Gateway         Flags Metric Ref    Use Iface
root@kali:~#
```

8. arp

```
File  Edit  View  Search  Terminal  Help
root@kali:~# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
reliance.reliance        ether   a8:da:0c:d6:48:bc   C                     wlan0
root@kali:~#
```

9. whois

```
File  Edit  View  Search  Terminal  Help
root@kali:~# whois facebook.com
   Domain Name: FACEBOOK.COM
   Registry Domain ID: 2320948_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrarsafe.com
   Registrar URL: http://www.registrarsafe.com
   Updated Date: 2022-01-26T16:45:06Z
   Creation Date: 1997-03-29T05:00:00Z
   Registry Expiry Date: 2031-03-30T04:00:00Z
   Registrar: RegistrarSafe, LLC
   Registrar IANA ID: 3237
   Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
   Registrar Abuse Contact Phone: +1-650-308-7004
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: A.NS.FACEBOOK.COM
   Name Server: B.NS.FACEBOOK.COM
   Name Server: C.NS.FACEBOOK.COM
   Name Server: D.NS.FACEBOOK.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-11-23T18:01:57Z <<<
```

10. ping

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ping www.google.com
PING www.google.com(maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004)) 56 data bytes
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=1 ttl=59 time=18.8 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=2 ttl=59 time=18.8 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=3 ttl=59 time=18.2 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=4 ttl=59 time=18.6 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=5 ttl=59 time=18.4 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=6 ttl=59 time=18.8 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=7 ttl=59 time=18.7 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=8 ttl=59 time=26.6 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=9 ttl=59 time=19.6 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=10 ttl=59 time=19.7 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=11 ttl=59 time=19.3 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=12 ttl=59 time=25.2 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=13 ttl=59 time=23.7 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=14 ttl=59 time=29.8 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=15 ttl=59 time=34.8 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=16 ttl=59 time=27.7 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=17 ttl=59 time=27.5 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=18 ttl=59 time=21.9 ms
64 bytes from maa05s20-in-x04.1e100.net (2404:6800:4007:81b::2004): icmp_seq=19 ttl=59 time=31.9 ms
^C
--- www.google.com ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 18038ms
rtt min/avg/max/mdev = 18.239/23.055/34.818/5.117 ms
root@kali:~#
```

11. curl wget

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# curl -0 www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf
root@kali:~# wget www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf
--2022-11-23 23:29:33--  http://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf
Resolving www.ftc.gov (www.ftc.gov)... 2405:200:1630:4ad::2031, 2405:200:1630:48a::2031, 23.214.240.64
Connecting to www.ftc.gov (www.ftc.gov)|2405:200:1630:4ad::2031|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf [following]
--2022-11-23 23:29:33--  https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf
Connecting to www.ftc.gov (www.ftc.gov)|2405:200:1630:4ad::2031|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3101899 (3.0M) [application/pdf]
Saving to: ‘cybersecuirty_sb_factsheets_all.pdf’

cybersecuirty_sb_factsheets_all.pdf               100%[=============================================================================================================>]   2.96M  --.-KB/s    in 0.1s

2022-11-23 23:29:33 (23.0 MB/s) - ‘cybersecuirty_sb_factsheets_all.pdf’ saved [3101899/3101899]

root@kali:~#
```

12. host

```
File  Edit  View  Search  Terminal  Help
root@kali:~# host google.com
google.com has address 142.250.195.46
google.com has IPv6 address 2404:6800:4007:822::200e
google.com mail is handled by 10 smtp.google.com.
root@kali:~# host amazon.com
amazon.com has address 52.94.236.248
amazon.com has address 54.239.28.85
amazon.com has address 205.251.242.103
amazon.com mail is handled by 5 amazon-smtp.amazon.com.
root@kali:~#
```

13. hostname

```
File  Edit  View  Search  Terminal  Help
root@kali:~# hostname
kali
root@kali:~# sudo hostname Cypher
root@kali:~# hostname
Cypher
root@kali:~#
```

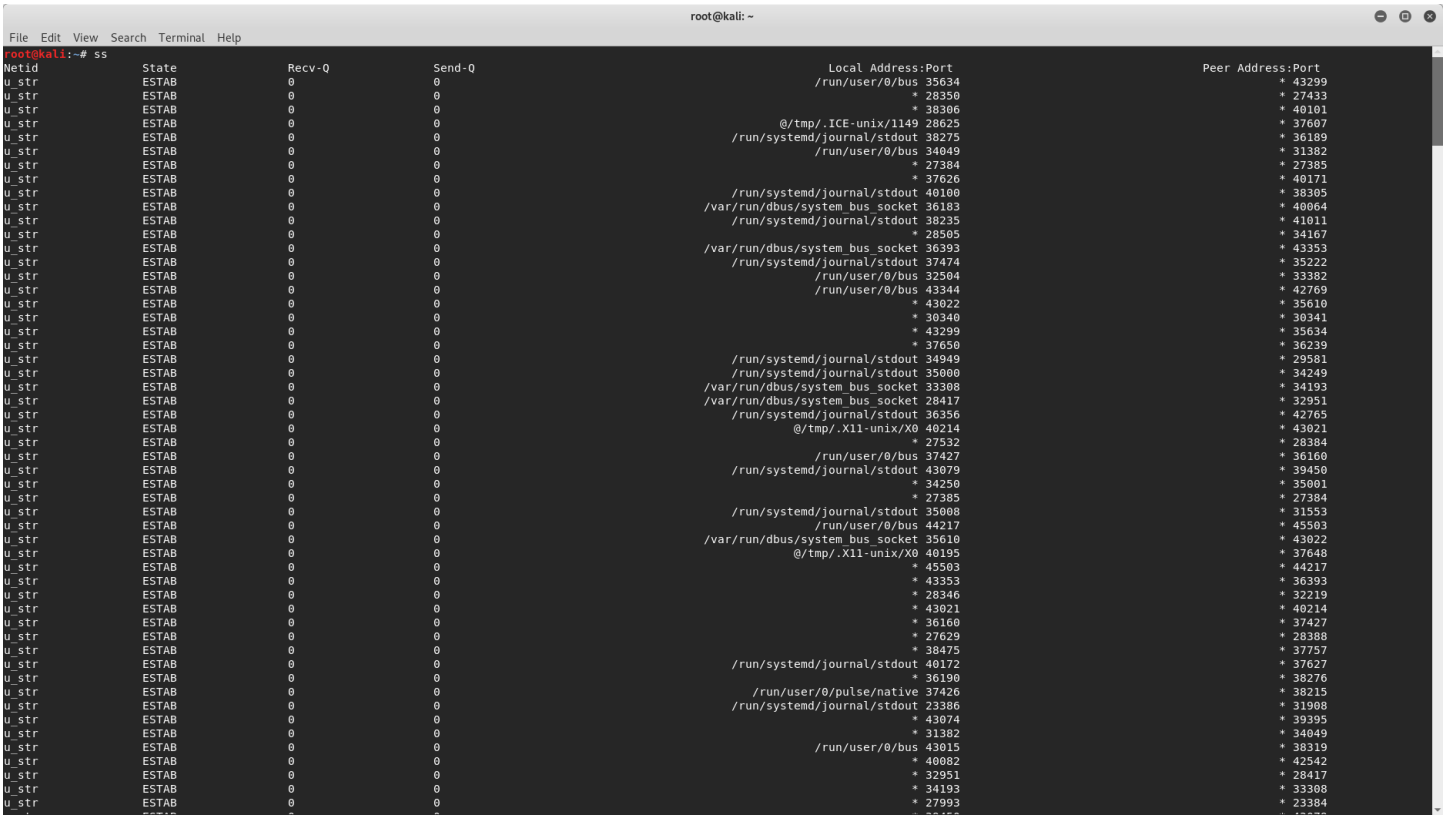
14. iwconfig

```
File  Edit  View  Search  Terminal  Help
root@kali:~# iwconfig
wlan0     IEEE 802.11  ESSID:"Shetty_5G"
          Mode:Managed  Frequency:5.18 GHz  Access Point: A8:DA:0C:D6:48:BE
          Bit Rate=866.7 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
          Link Quality=70/70  Signal level=-27 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:7   Missed beacon:0

lo        no wireless extensions.

root@kali:~#
```

15. tcpdump

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), capture size 262144 bytes
23:35:07.929546 IP 192.168.29.243.56296 > 192.168.29.255.5775: UDP, length 42
23:35:07.930723 IP kali.54911 > reliance.reliance.domain: 53248+ PTR? 255.29.168.192.in-addr.arpa. (45)
23:35:07.933124 IP reliance.reliance.domain > kali.54911: 53248 NXDomain 0/0/0 (45)
23:35:07.934104 IP kali.58061 > reliance.reliance.domain: 24853+ PTR? 243.29.168.192.in-addr.arpa. (45)
23:35:07.935434 IP reliance.reliance.domain > kali.58061: 24853 NXDomain 0/0/0 (45)
23:35:07.936081 IP kali.53579 > reliance.reliance.domain: 30550+ PTR? 1.29.168.192.in-addr.arpa. (43)
23:35:07.937319 IP reliance.reliance.domain > kali.53579: 30550* 1/0/0 PTR reliance.reliance. (74)
23:35:07.937624 IP kali.58079 > reliance.reliance.domain: 21924+ PTR? 33.29.168.192.in-addr.arpa. (44)
23:35:07.938891 IP reliance.reliance.domain > kali.58079: 21924 NXDomain 0/0/0 (44)
23:35:09.977524 IP 192.168.29.243.56296 > 192.168.29.255.5775: UDP, length 42
23:35:10.796689 IP reliance.reliance > all-systems.mcast.net: igmp query v3
23:35:10.796999 IP kali.38160 > reliance.reliance.domain: 26986+ PTR? 1.0.0.224.in-addr.arpa. (40)
23:35:10.799715 IP reliance.reliance.domain > kali.38160: 26986 1/0/0 PTR all-systems.mcast.net. (75)
23:35:12.230291 IP 192.168.29.243.56296 > 192.168.29.255.5775: UDP, length 42
23:35:12.640045 ARP, Request who-has 192.168.29.243 (Broadcast) tell reliance.reliance, length 28
23:35:14.278373 IP 192.168.29.243.56296 > 192.168.29.255.5775: UDP, length 42
23:35:14.688063 ARP, Request who-has kali (Broadcast) tell reliance.reliance, length 28
23:35:14.688091 ARP, Reply kali is-at b4:69:21:d3:07:a7 (oui Unknown), length 28
23:35:15.712369 ARP, Request who-has kali (b4:69:21:d3:07:a7 (oui Unknown)) tell reliance.reliance, length 28
23:35:15.712398 ARP, Reply kali is-at b4:69:21:d3:07:a7 (oui Unknown), length 28
23:35:15.909198 ARP, Request who-has reliance.reliance tell kali, length 28
23:35:15.910481 ARP, Reply reliance.reliance is-at a8:da:0c:d6:48:bc (oui Unknown), length 28
23:35:16.326238 IP 192.168.29.243.56296 > 192.168.29.255.5775: UDP, length 42
23:35:16.736093 ARP, Request who-has 192.168.29.242 (Broadcast) tell reliance.reliance, length 28
23:35:16.736349 IP kali.43105 > reliance.reliance.domain: 38311+ PTR? 242.29.168.192.in-addr.arpa. (45)
23:35:16.751614 IP reliance.reliance.domain > kali.43105: 38311 NXDomain* 0/1/0 (104)
23:35:18.169773 IP6  gateway > ip6-allnodes: ICMP6, router advertisement, length 88
23:35:18.170116 IP kali.38962 > reliance.reliance.domain: 17455+ PTR? c.b.0.4.6.d.e.f.f.f.c.0.a.d.a.a.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
23:35:18.172714 IP reliance.reliance.domain > kali.38962: 17455 NXDomain 0/0/0 (90)
23:35:18.180938 IP6 kali > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
23:35:18.181188 IP kali.37379 > reliance.reliance.domain: 45653+ PTR? 6.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
23:35:18.189550 IP reliance.reliance.domain > kali.37379: 45653 NXDomain 0/0/0 (90)
23:35:18.190163 IP kali.53719 > reliance.reliance.domain: 20250+ PTR? 0.1.d.0.6.6.5.9.b.0.6.0.6.c.e.d.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
23:35:18.192176 IP reliance.reliance.domain > kali.53719: 20250 NXDomain 0/0/0 (90)
23:35:18.421171 IP6 kali > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
23:35:18.579380 IP 192.168.29.243.56296 > 192.168.29.255.5775: UDP, length 42
23:35:20.422571 IP 192.168.29.243.56296 > 192.168.29.255.5775: UDP, length 42
23:35:22.470644 IP 192.168.29.243.56296 > 192.168.29.255.5775: UDP, length 42
23:35:24.518644 IP 192.168.29.243.56296 > 192.168.29.255.5775: UDP, length 42
23:35:26.566775 IP 192.168.29.243.56296 > 192.168.29.255.5775: UDP, length 42
23:35:28.614767 IP 192.168.29.243.56296 > 192.168.29.255.5775: UDP, length 42
23:35:30.662772 IP 192.168.29.243.56296 > 192.168.29.255.5775: UDP, length 42
23:35:30.867414 IP reliance.reliance > all-systems.mcast.net: igmp query v3
23:35:31.401913 IP6  gateway > ip6-allnodes: ICMP6, router advertisement, length 88
23:35:31.492931 IP6 kali > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
23:35:31.677201 IP6 kali > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
^C
46 packets captured
46 packets received by filter
0 packets dropped by kernel
root@kali:~#
```

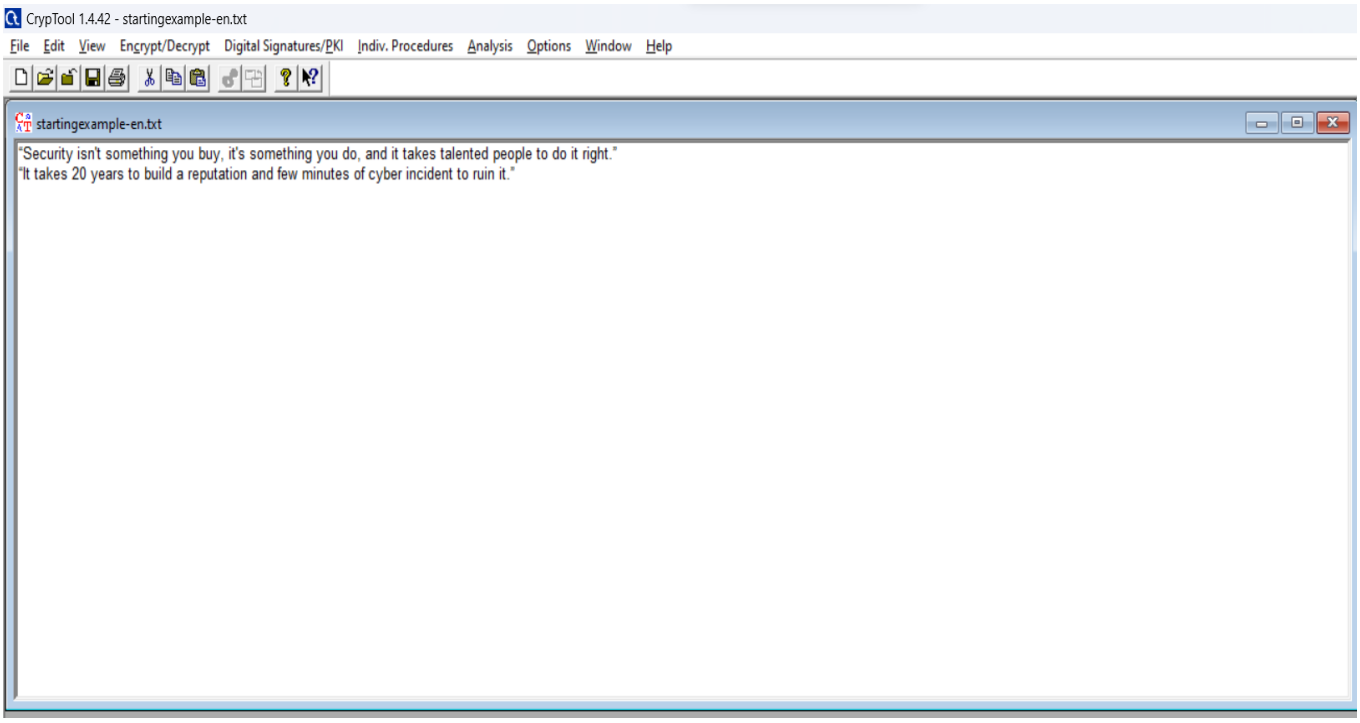
16. ss


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ss
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port
u_str ESTAB 0 0 /run/user/0/bus 35634 * 43299
u_str ESTAB 0 0 * 28350 * 27433
u_str ESTAB 0 0 * 38306 * 40101
u_str ESTAB 0 0 @/tmp/.ICE-unix/1149 28625 * 37607
u_str ESTAB 0 0 /run/systemd/journal/stdout 38275 * 36189
u_str ESTAB 0 0 /run/user/0/bus 34049 * 31382
u_str ESTAB 0 0 * 27384 * 27385
u_str ESTAB 0 0 * 37626 * 40171
u_str ESTAB 0 0 /run/systemd/journal/stdout 40100 * 38305
u_str ESTAB 0 0 /var/run/dbus/system_bus_socket 36183 * 40064
u_str ESTAB 0 0 /run/systemd/journal/stdout 38235 * 41011
u_str ESTAB 0 0 * 28505 * 34167
u_str ESTAB 0 0 /var/run/dbus/system_bus_socket 36393 * 43353
u_str ESTAB 0 0 /run/systemd/journal/stdout 37474 * 35222
u_str ESTAB 0 0 /run/user/0/bus 32504 * 33382
u_str ESTAB 0 0 /run/user/0/bus 43344 * 42769
u_str ESTAB 0 0 * 43022 * 35610
u_str ESTAB 0 0 * 30340 * 30341
u_str ESTAB 0 0 * 43299 * 35634
u_str ESTAB 0 0 * 37650 * 36239
u_str ESTAB 0 0 /run/systemd/journal/stdout 34949 * 29581
u_str ESTAB 0 0 /run/systemd/journal/stdout 35000 * 34249
u_str ESTAB 0 0 /var/run/dbus/system_bus_socket 33308 * 34193
u_str ESTAB 0 0 /var/run/dbus/system_bus_socket 28417 * 32951
u_str ESTAB 0 0 /run/systemd/journal/stdout 36356 * 42765
u_str ESTAB 0 0 @/tmp/.X11-unix/X0 40214 * 43021
u_str ESTAB 0 0 * 27532 * 28384
u_str ESTAB 0 0 /run/user/0/bus 37427 * 36160
u_str ESTAB 0 0 /run/systemd/journal/stdout 43079 * 39450
u_str ESTAB 0 0 * 34250 * 35001
u_str ESTAB 0 0 * 27385 * 27384
u_str ESTAB 0 0 /run/systemd/journal/stdout 35008 * 31553
u_str ESTAB 0 0 /run/user/0/bus 44217 * 45503
u_str ESTAB 0 0 /var/run/dbus/system_bus_socket 35610 * 43022
u_str ESTAB 0 0 @/tmp/.X11-unix/X0 40195 * 37648
u_str ESTAB 0 0 * 45503 * 44217
u_str ESTAB 0 0 * 43353 * 36393
u_str ESTAB 0 0 * 28346 * 32219
u_str ESTAB 0 0 * 43021 * 40214
u_str ESTAB 0 0 * 36160 * 37427
u_str ESTAB 0 0 * 27629 * 28388
u_str ESTAB 0 0 * 38475 * 37757
u_str ESTAB 0 0 /run/systemd/journal/stdout 40172 * 37627
u_str ESTAB 0 0 * 36190 * 38276
u_str ESTAB 0 0 /run/user/0/pulse/native 37426 * 38215
u_str ESTAB 0 0 /run/systemd/journal/stdout 23386 * 31908
u_str ESTAB 0 0 * 43074 * 39395
u_str ESTAB 0 0 * 31382 * 34049
u_str ESTAB 0 0 /run/user/0/bus 43015 * 38319
u_str ESTAB 0 0 * 40082 * 42542
u_str ESTAB 0 0 * 32951 * 28417
u_str ESTAB 0 0 * 34193 * 33308
u_str ESTAB 0 0 * 27993 * 23384

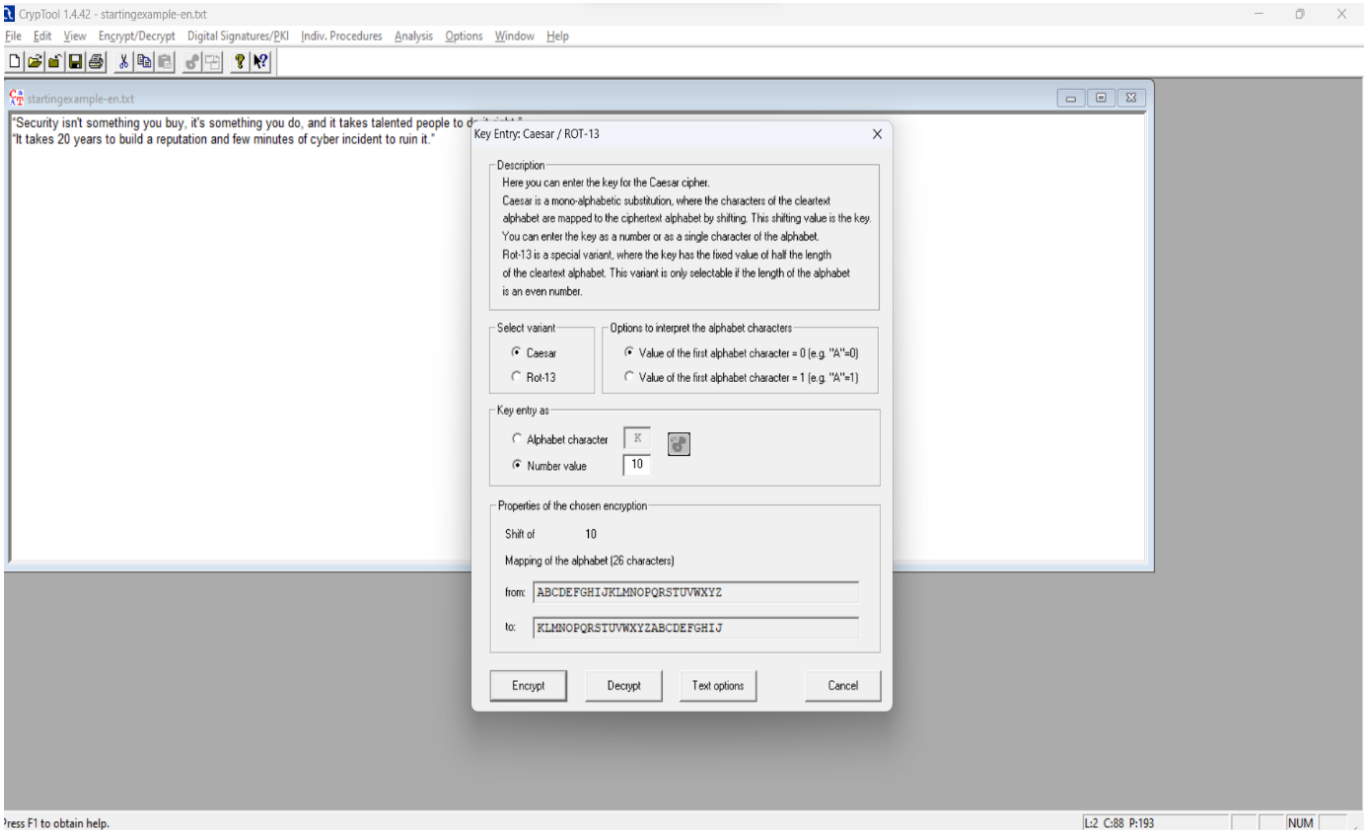
Assignment – 3

Activity – 1

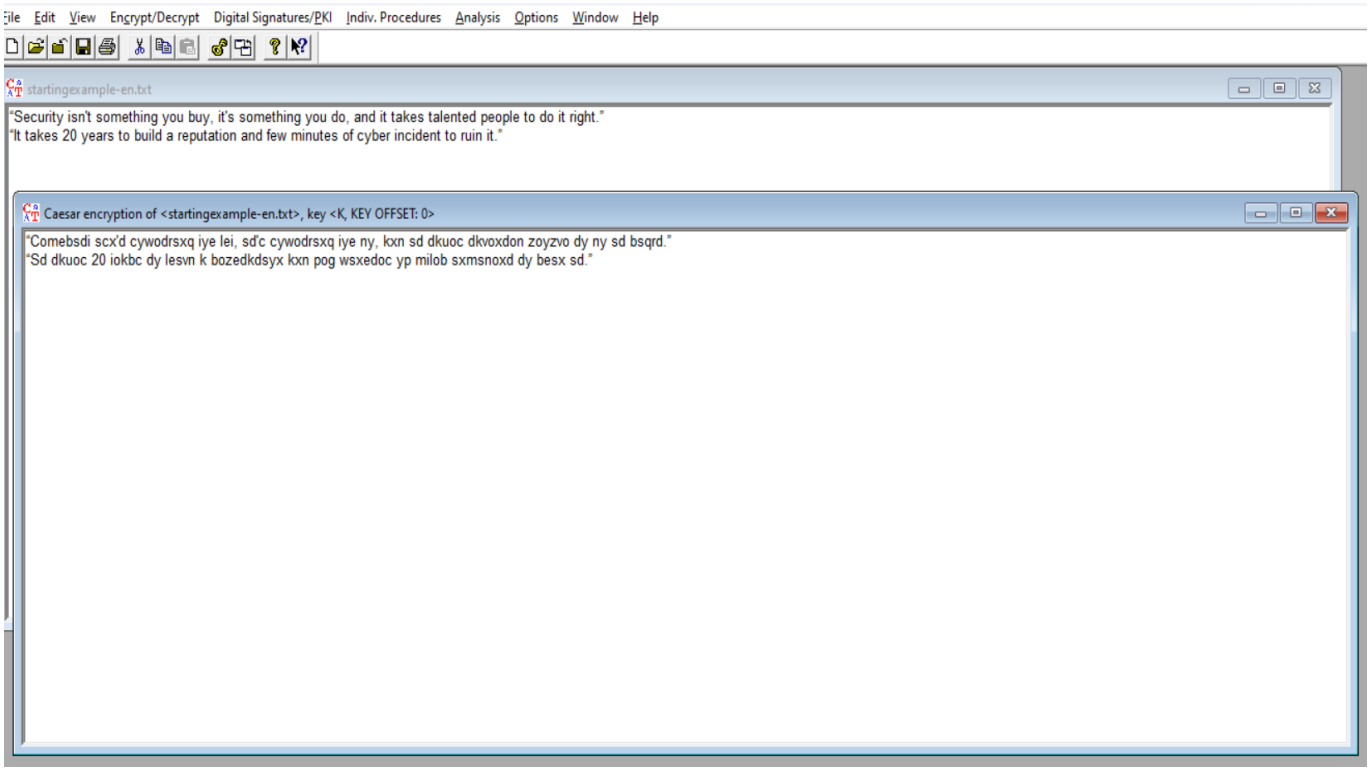
Text Message



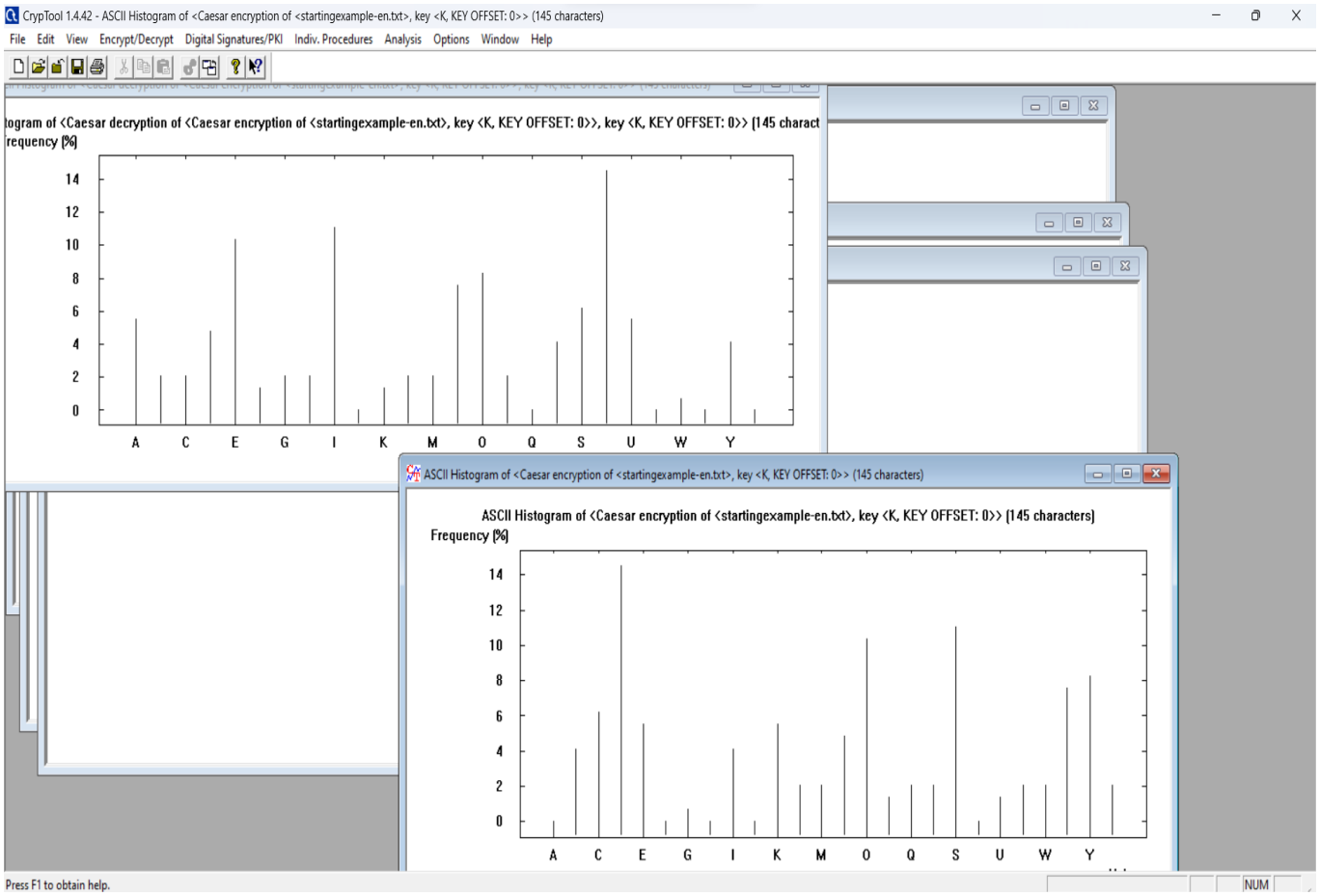
Encryption Number Value



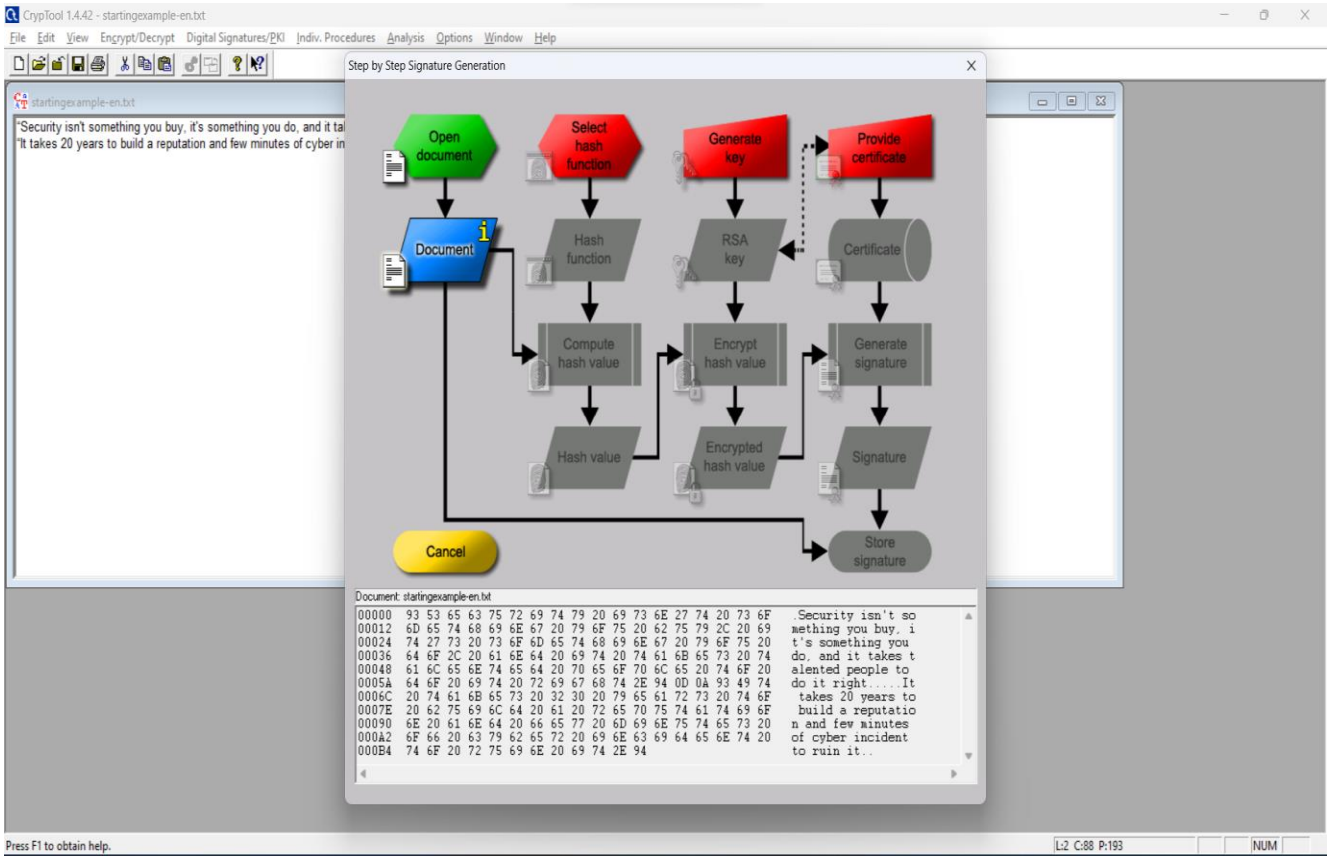
Encrypted Form of Message

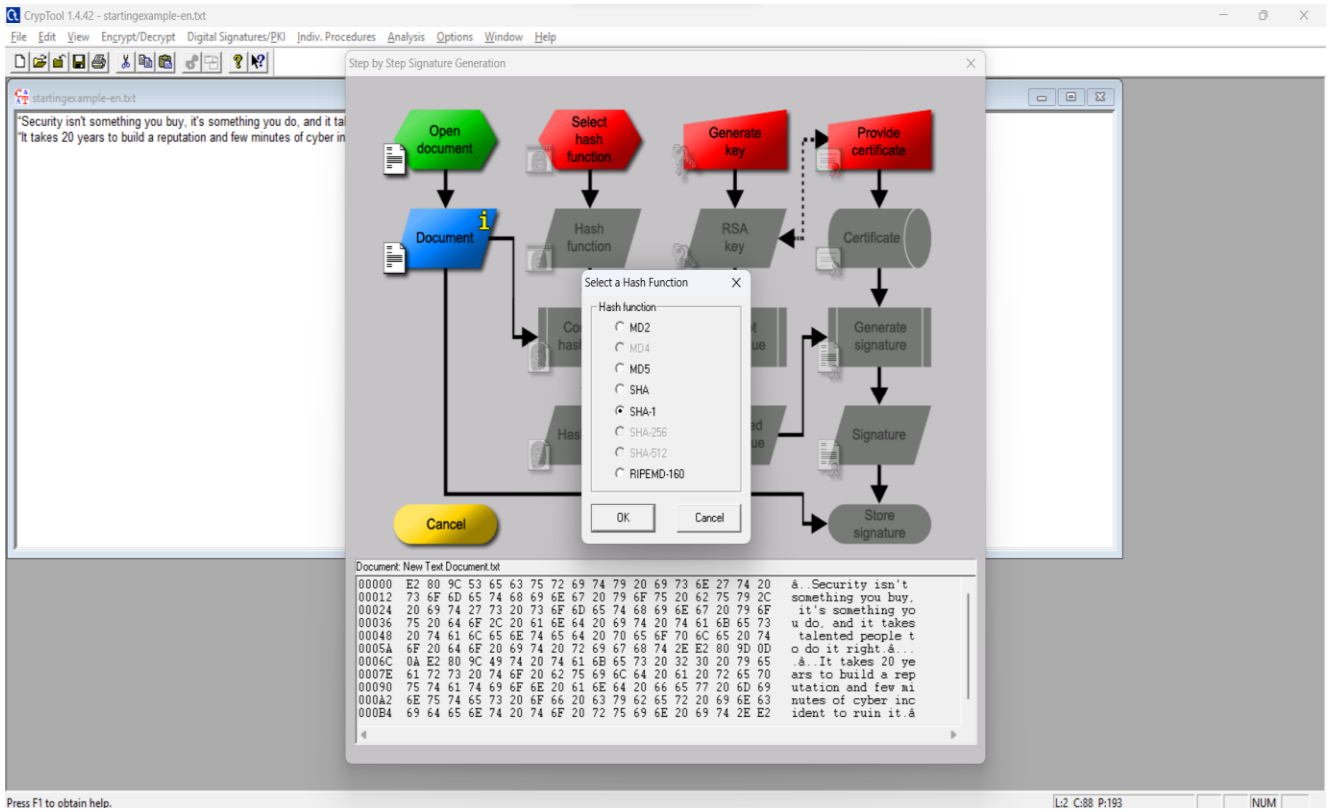


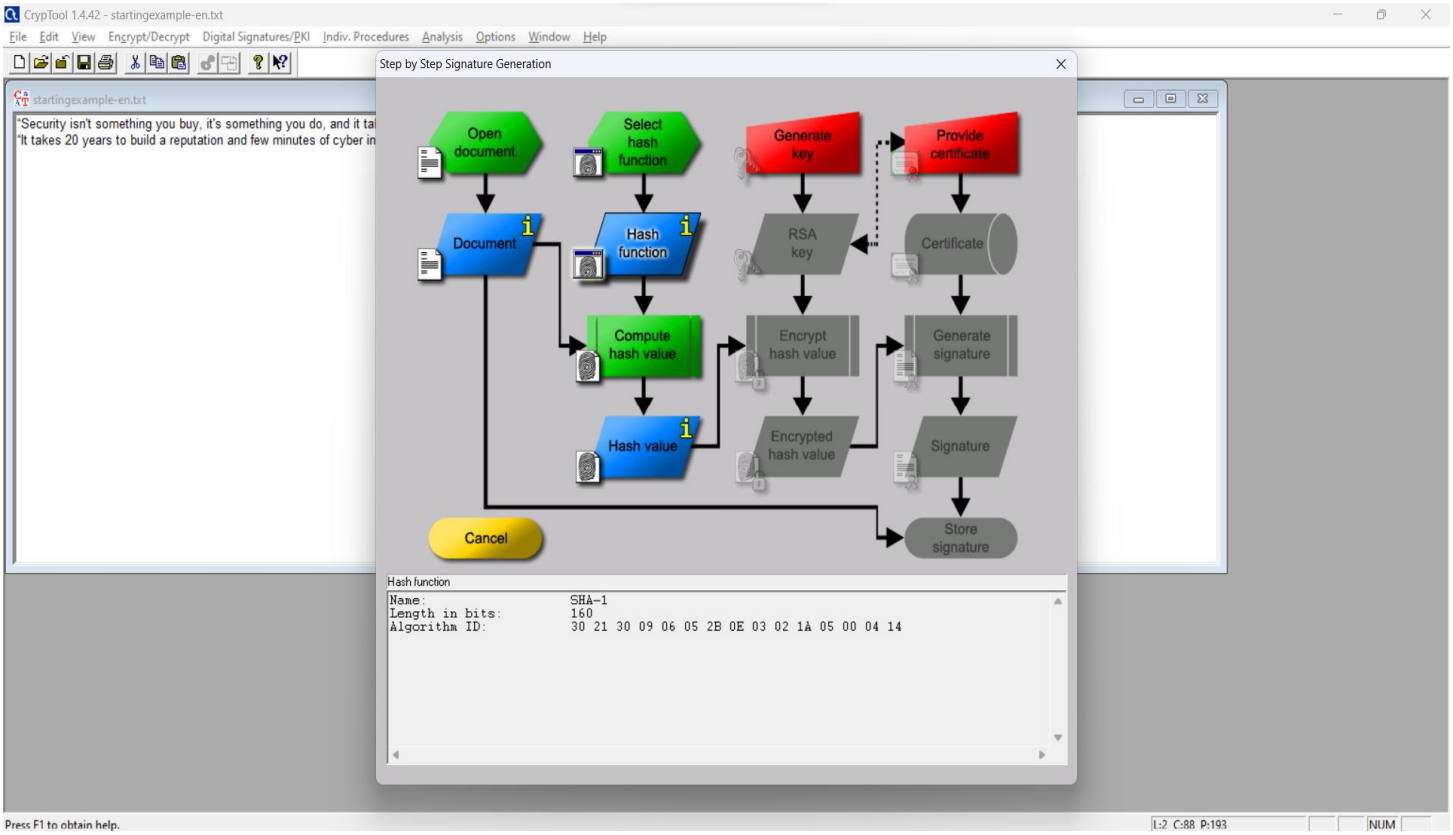
Encryption vs Decryption Histogram

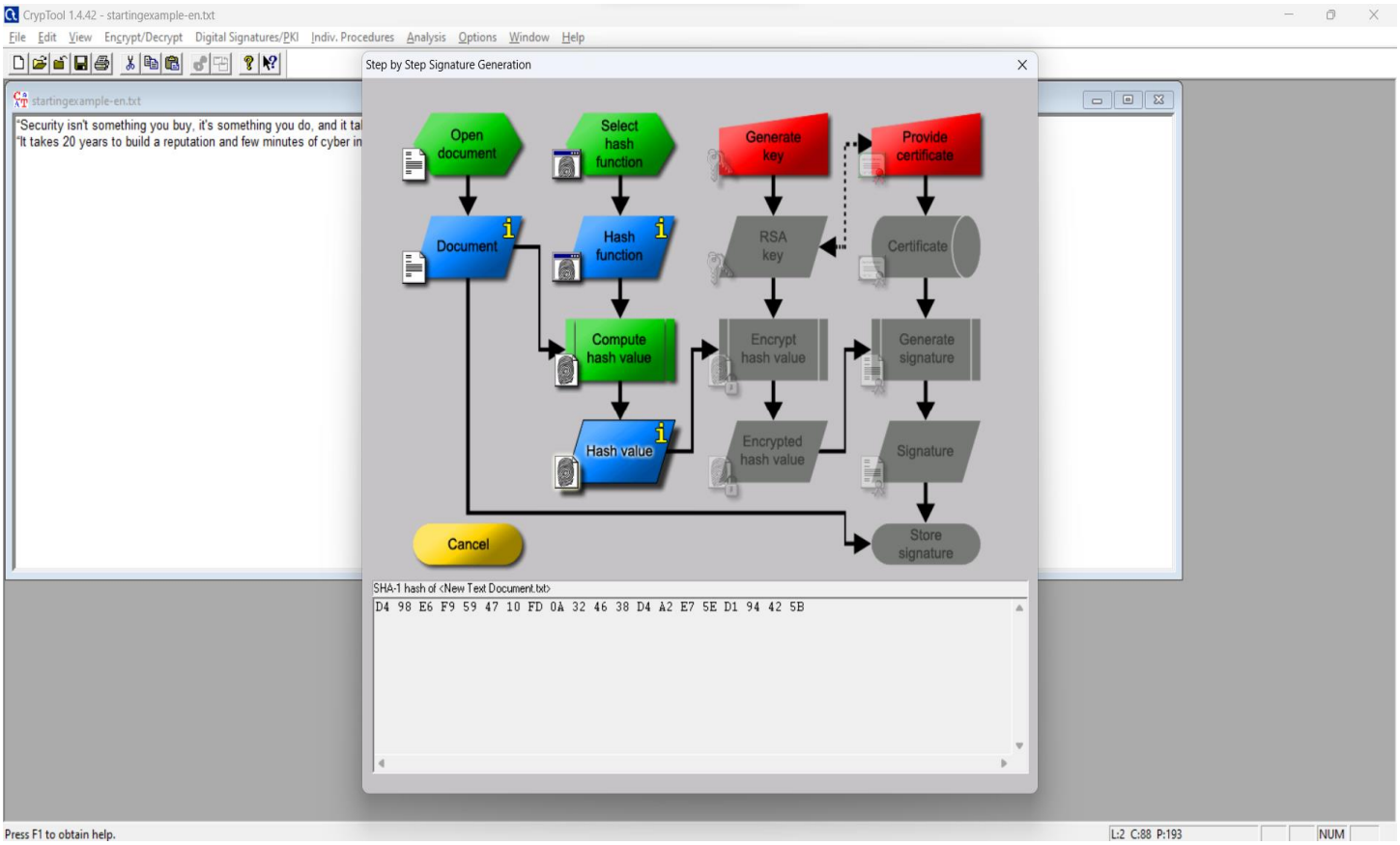


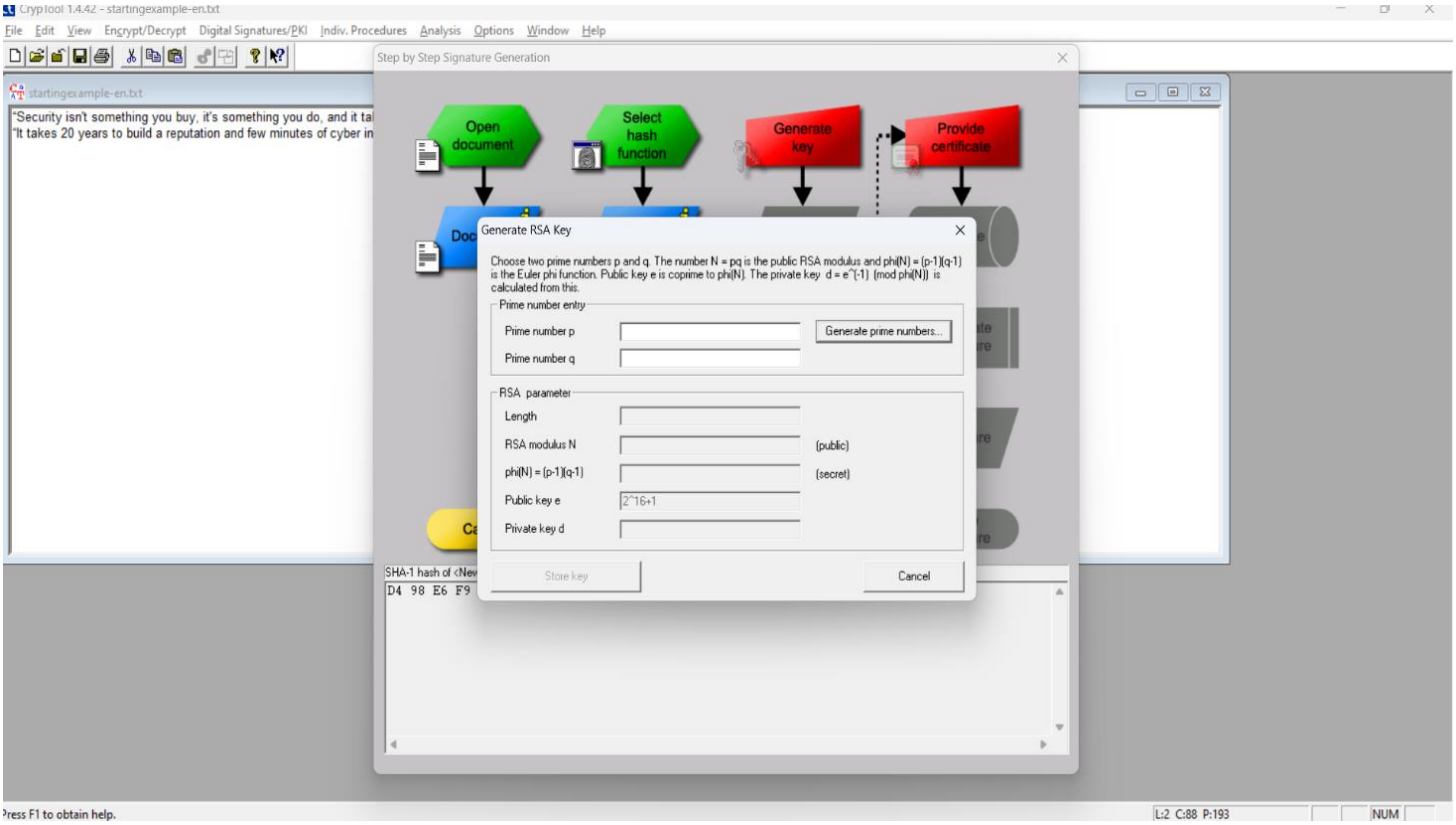
Digital Signature Process

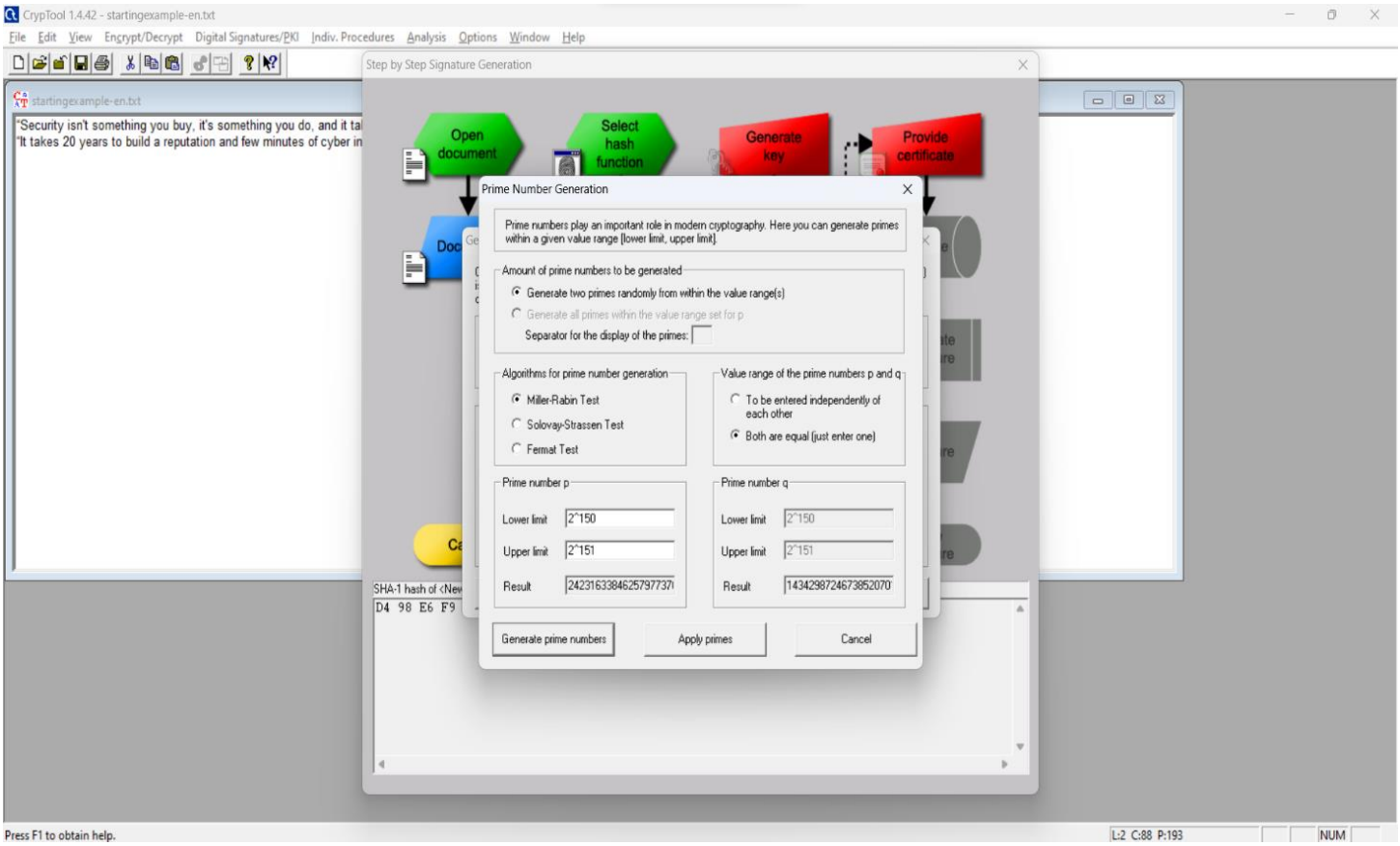


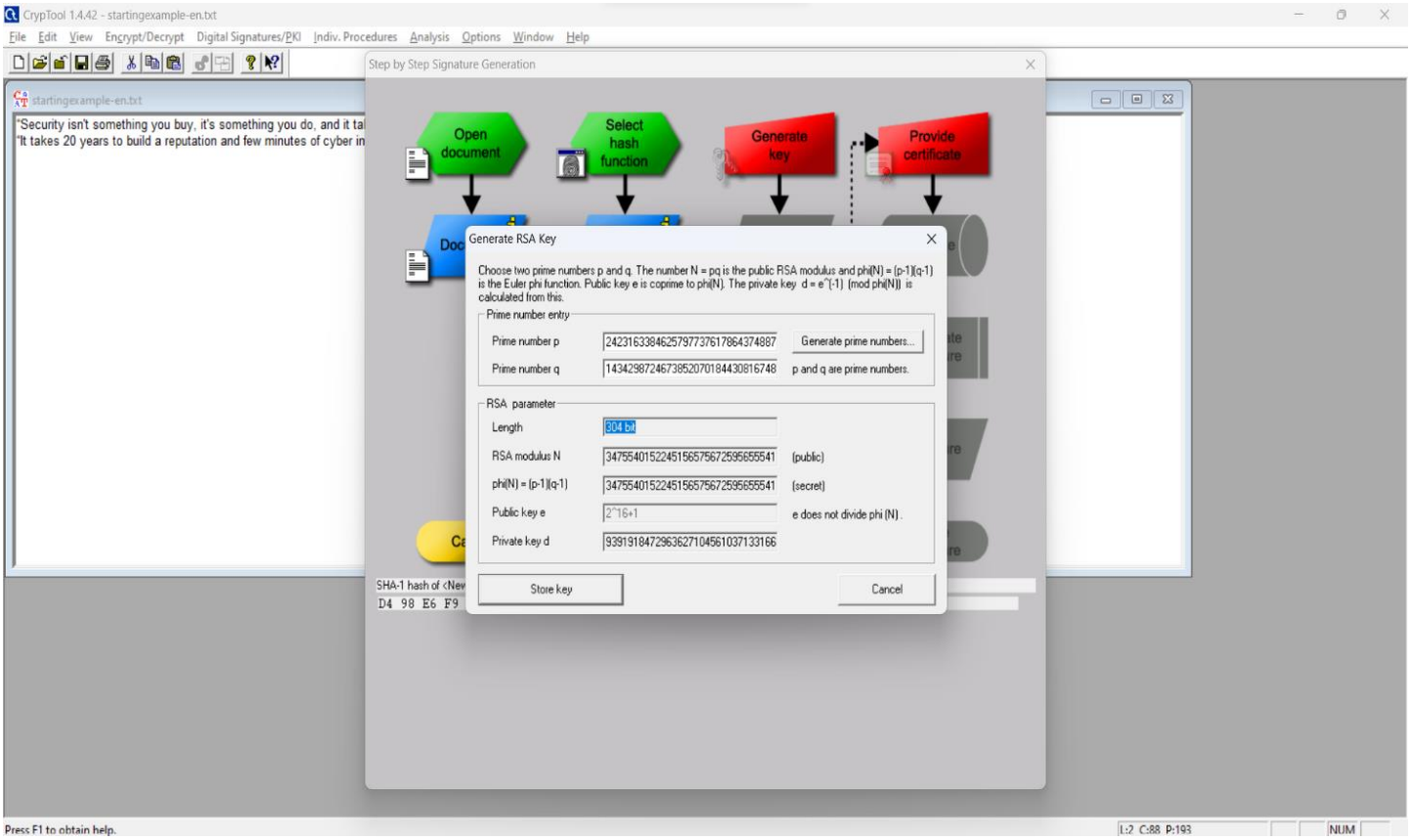


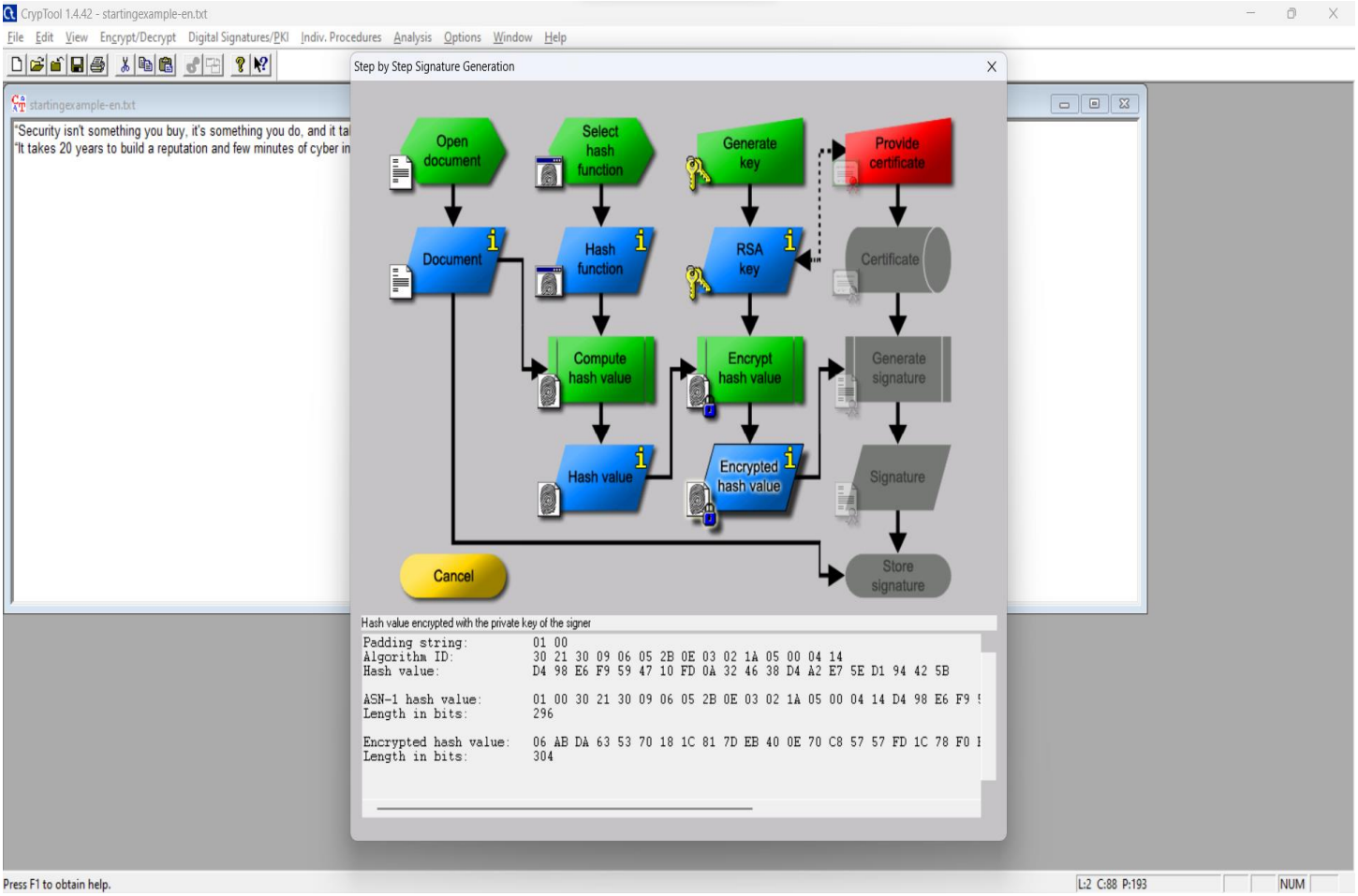

CrypTool 1.4.42 - startingexample-en.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en.txt
"Security isn't something you buy, it's something you do, and it tal
"It takes 20 years to build a reputation and few minutes of cyber in
Step by Step Signature Generation
Open document
Select hash function
Generate key
Provide certificate
Document
Hash function
RSA key
Certificate
Compute hash value
Encrypt hash value
Generate signature
Hash value
Encrypted hash value
Signature
Cancel
Store signature
Hash function
Name: SHA-1
Length in bits: 160
Algorithm ID: 30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14
Press F1 to obtain help.
L:2 C:88 P:193
NUM

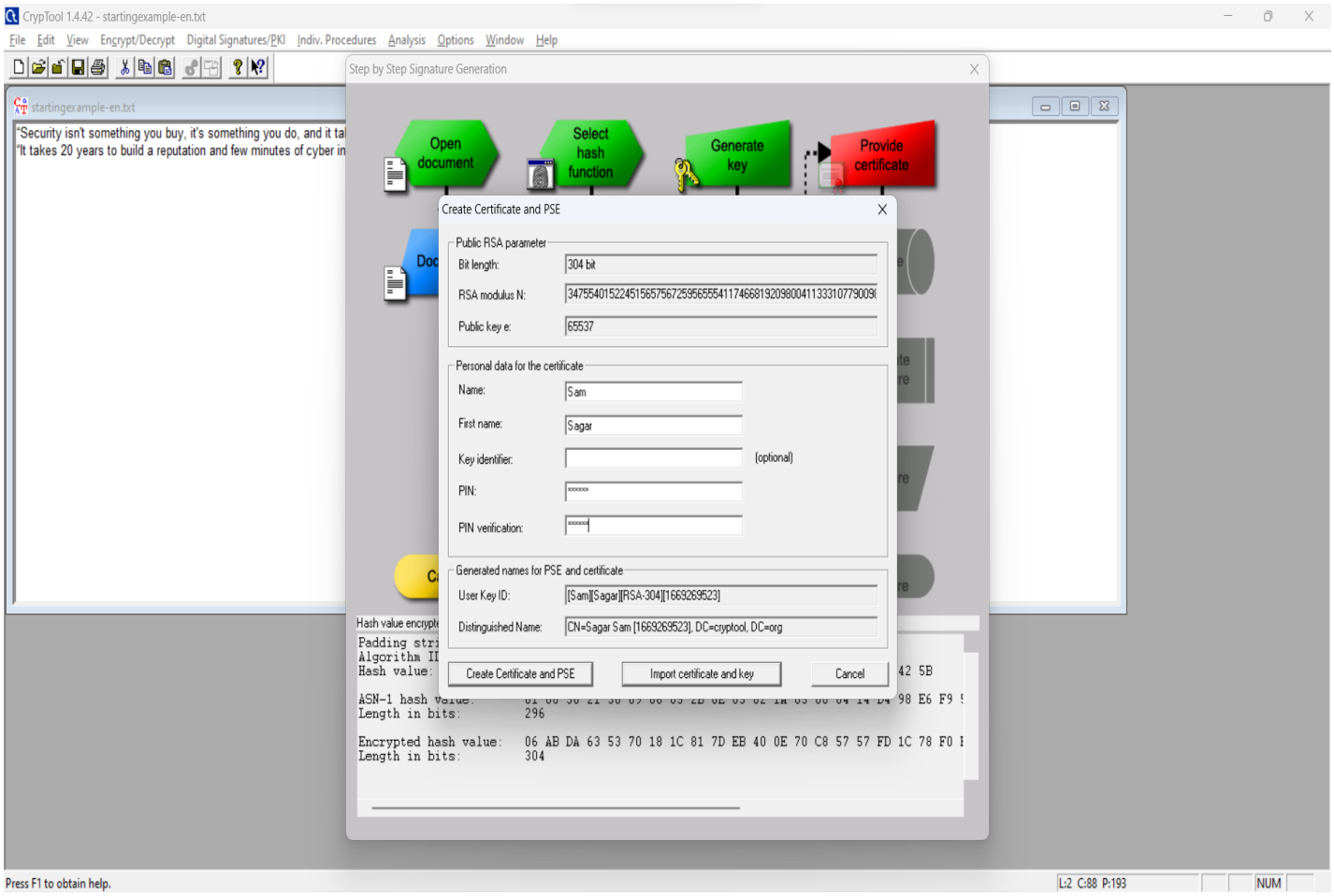

CrypTool 1.4.42 - startingexample-en.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en.txt
"Security isn't something you buy, it's something you do, and it tal
"It takes 20 years to build a reputation and few minutes of cyber in
Step by Step Signature Generation
Open document
Select hash function
Generate key
Provide certificate
Document
Hash function
RSA key
Certificate
Compute hash value
Encrypt hash value
Generate signature
Hash value
Encrypted hash value
Signature
Cancel
Store signature
SHA-1 hash of <New Text Document.txt>
D4 98 E6 F9 59 47 10 FD 0A 32 46 38 D4 A2 E7 5E D1 94 42 5B
Press F1 to obtain help.
L:2 C:88 P:193
NUM

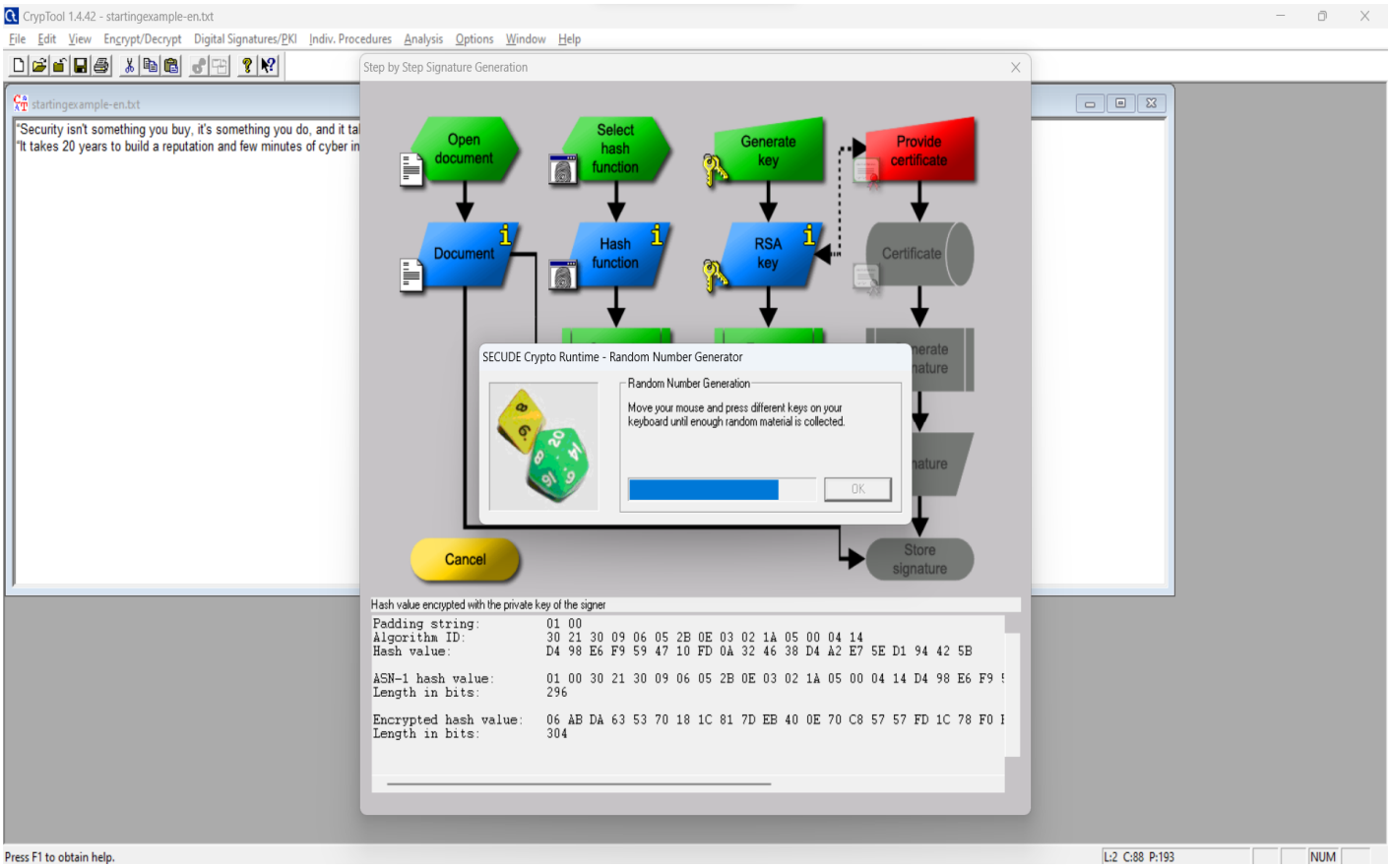

CrypTool 1.4.42 - startingexample-en.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Step by Step Signature Generation
Open document
Select hash function
Generate key
Provide certificate
Generate RSA Key
Choose two prime numbers p and q. The number N = pq is the public RSA modulus and phi(N) = (p-1)(q-1) is the Euler phi function. Public key e is coprime to phi(N). The private key d = e^(-1) (mod phi(N)) is calculated from this.
Prime number entry
Prime number p
Prime number q
Generate prime numbers...
RSA parameter
Length
RSA modulus N
(public)
phi(N) = (p-1)(q-1)
(secret)
Public key e
2^16+1
Private key d
Store key
Cancel
SHA-1 hash of
D4 98 E6 F9
Press F1 to obtain help.
L:2 C:88 P:193
NUM

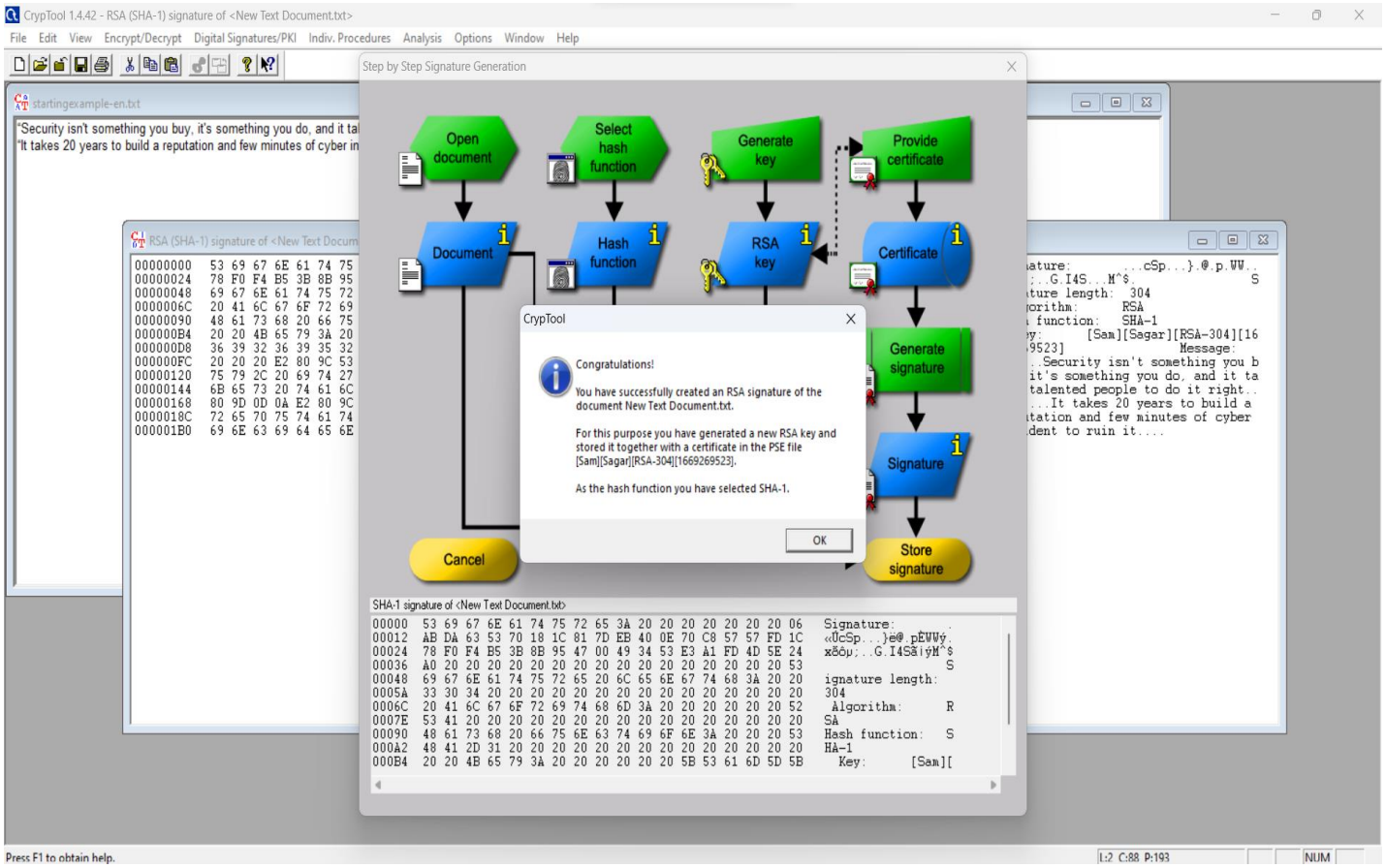

CrypTool 1.4.42 - startingexample-en.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Step by Step Signature Generation
Open document
Select hash function
Generate key
Provide certificate
Prime Number Generation
Prime numbers play an important role in modern cryptography. Here you can generate primes within a given value range [lower limit, upper limit].
Amount of prime numbers to be generated
Generate two primes randomly from within the value range(s)
Generate all primes within the value range set for p
Separator for the display of the primes:
Algorithms for prime number generation
Miller-Rabin Test
Solovay-Strassen Test
Fermat Test
Value range of the prime numbers p and q
To be entered independently of each other
Both are equal (just enter one)
Prime number p
Lower limit 2^150
Upper limit 2^151
Result 24231633846257977371
Prime number q
Lower limit 2^150
Upper limit 2^151
Result 1434298724673852070
Generate prime numbers
Apply primes
Cancel
SHA-1 hash of
D4 98 E6 F9
Press F1 to obtain help.
L:2 C:88 P:193
NUM

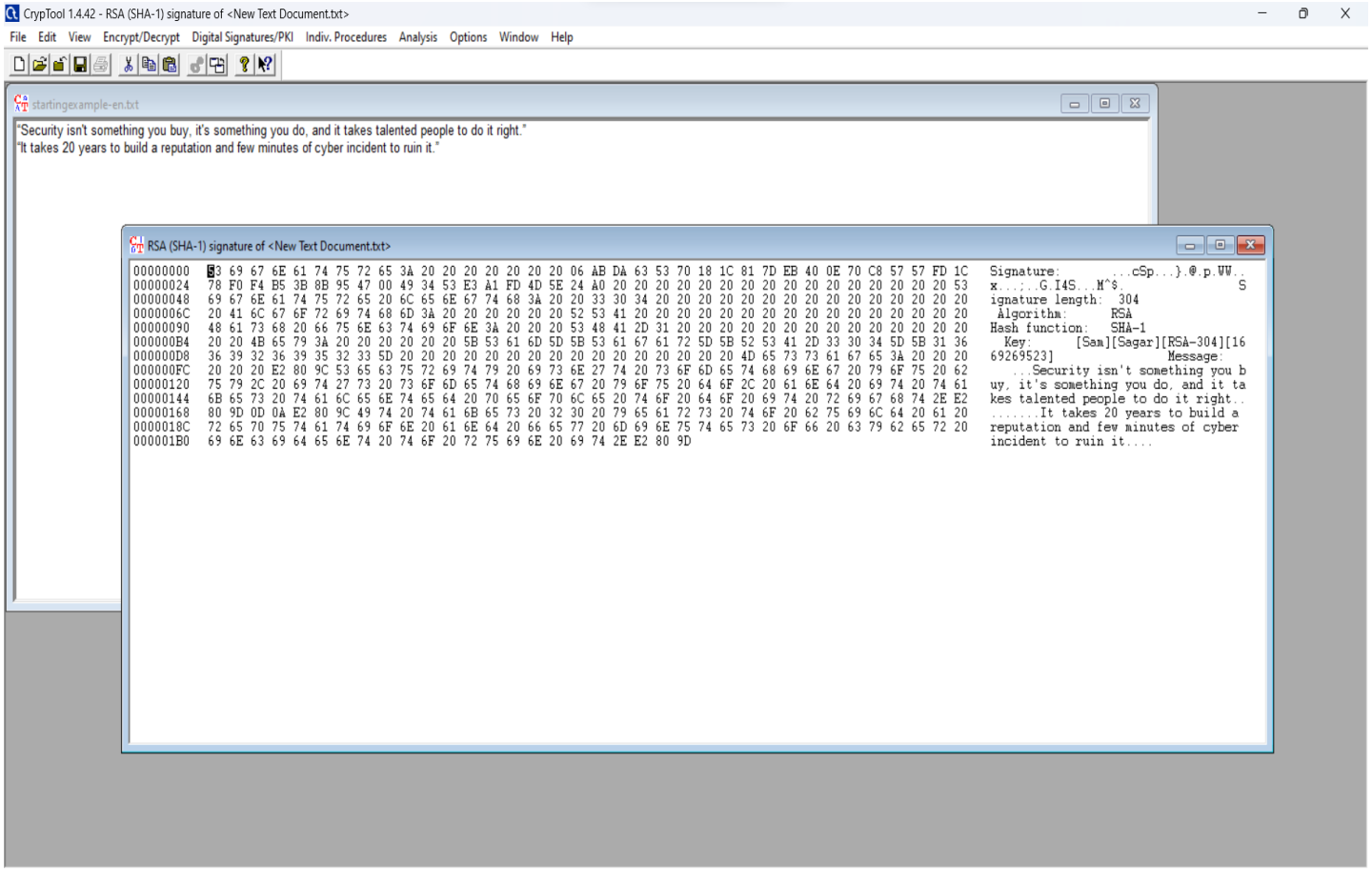

CrypTool 1.4.42 - startingexample-en.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en.txt
"Security isn't something you buy, it's something you do, and it tal
"It takes 20 years to build a reputation and few minutes of cyber in
Step by Step Signature Generation
Open document
Select hash function
Generate key
Provide certificate
Generate RSA Key
Choose two prime numbers p and q. The number N = pq is the public RSA modulus and phi(N) = (p-1)(q-1) is the Euler phi function. Public key e is coprime to phi(N). The private key d = e^(-1) (mod phi(N)) is calculated from this.
Prime number entry
Prime number p
24231633846257977376178643748 87
Generate prime numbers...
Prime number q
14342987246738520701844308167 48
p and q are prime numbers.
RSA parameter
Length
304 bit
RSA modulus N
34755401522451565756725956555 41
(public)
phi(N) = (p-1)(q-1)
34755401522451565756725956555 41
(secret)
Public key e
2^16+1
e does not divide phi (N).
Private key d
93919184729636271045610371331 66
Store key
Cancel
SHA-1 hash of <New
D4 98 E6 F9
Press F1 to obtain help.
L:2 C:88 P:193
NUM


CrypTool 1.4.42 - startingexample-en.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en.txt
"Security isn't something you buy, it's something you do, and it tal
"It takes 20 years to build a reputation and few minutes of cyber in
Step by Step Signature Generation
Open document
Select hash function
Generate key
Provide certificate
Document
Hash function
RSA key
Certificate
Compute hash value
Encrypt hash value
Generate signature
Hash value
Encrypted hash value
Signature
Cancel
Store signature
Hash value encrypted with the private key of the signer
Padding string: 01 00
Algorithm ID: 30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14
Hash value: D4 98 E6 F9 59 47 10 FD 0A 32 46 38 D4 A2 E7 5E D1 94 42 5B
ASN-1 hash value: 01 00 30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14 D4 98 E6 F9
Length in bits: 296
Encrypted hash value: 06 AB DA 63 53 70 18 1C 81 7D EB 40 0E 70 C8 57 57 FD 1C 78 F0
Length in bits: 304
Press F1 to obtain help.
L:2 C:88 P:193
NUM


CrypTool 1.4.42 - startingexample-en.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Step by Step Signature Generation
startingexample-en.txt
"Security isn't something you buy, it's something you do, and it tal
"It takes 20 years to build a reputation and few minutes of cyber in
Open document
Select hash function
Generate key
Provide certificate
Create Certificate and PSE
Public RSA parameter
Bit length: 304 bit
RSA modulus N:
Public key e: 65537
Personal data for the certificate
Name: Sam
First name: Sagar
Key identifier:
(optional)
PIN:
PIN verification:
Generated names for PSE and certificate
User Key ID: [Sam][Sagar][RSA-304][1669269523]
Distinguished Name: CN=Sagar Sam [1669269523], DC=cryptool, DC=org
Create Certificate and PSE
Import certificate and key
Cancel
Hash value encrypte
Padding stri
Algorithm ID
Hash value:
ASN-1 hash value:
Length in bits: 296
Encrypted hash value: 06 AB DA 63 53 70 18 1C 81 7D EB 40 0E 70 C8 57 57 FD 1C 78 F0
Length in bits: 304
Press F1 to obtain help.
L:2 C:88 P:193
NUM


CrypTool 1.4.42 - startingexample-en.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Step by Step Signature Generation
startingexample-en.txt
"Security isn't something you buy, it's something you do, and it tal
"It takes 20 years to build a reputation and few minutes of cyber in
Open document
Select hash function
Generate key
Provide certificate
Document
Hash function
RSA key
Certificate
SECUDE Crypto Runtime - Random Number Generator
Random Number Generation
Move your mouse and press different keys on your keyboard until enough random material is collected.
OK
Cancel
Store signature
Hash value encrypted with the private key of the signer
Padding string: 01 00
Algorithm ID: 30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14
Hash value: D4 98 E6 F9 59 47 10 FD 0A 32 46 38 D4 A2 E7 5E D1 94 42 5B
ASN-1 hash value: 01 00 30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14 D4 98 E6 F9
Length in bits: 296
Encrypted hash value: 06 AB DA 63 53 70 18 1C 81 7D EB 40 0E 70 C8 57 57 FD 1C 78 F0
Length in bits: 304
Press F1 to obtain help.
L:2 C:88 P:193
NUM


CrypTool 1.4.42 - RSA (SHA-1) signature of <New Text Document.txt>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Step by Step Signature Generation
Open document
Select hash function
Generate key
Provide certificate
Document
Hash function
RSA key
Certificate
Generate signature
Signature
Store signature
Cancel
CrypTool
Congratulations!
You have successfully created an RSA signature of the document New Text Document.txt.
For this purpose you have generated a new RSA key and stored it together with a certificate in the PSE file [Sam][Sagar][RSA-304][1669269523].
As the hash function you have selected SHA-1.
OK
SHA-1 signature of <New Text Document.txt>
Press F1 to obtain help.
NUM


CrypTool 1.4.42 - RSA (SHA-1) signature of <New Text Document.txt>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en.txt
"Security isn't something you buy, it's something you do, and it takes talented people to do it right."
"It takes 20 years to build a reputation and few minutes of cyber incident to ruin it."
RSA (SHA-1) signature of <New Text Document.txt>

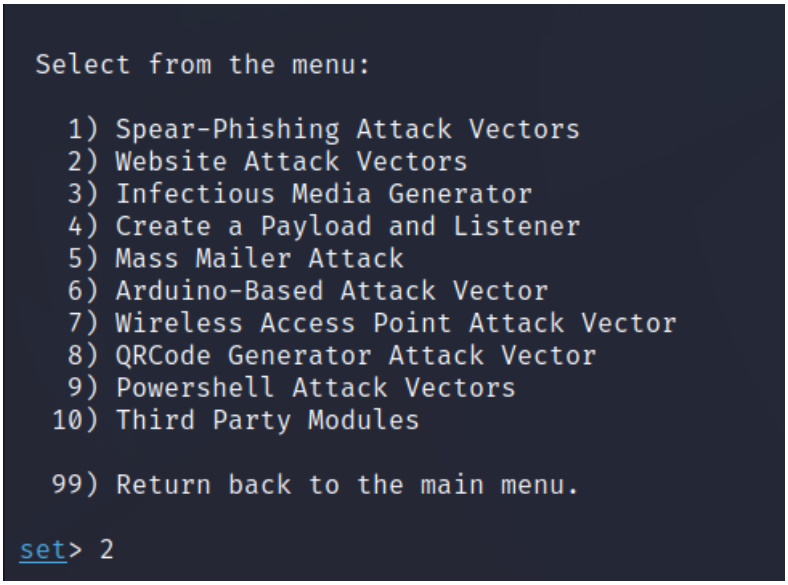
Assignment-4

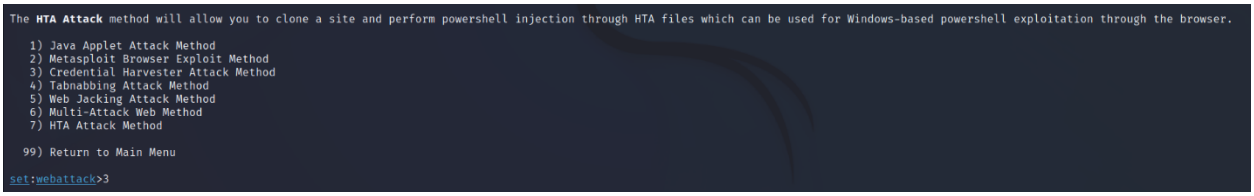
Activity-1: Clone Google and Twitter homepage using set.

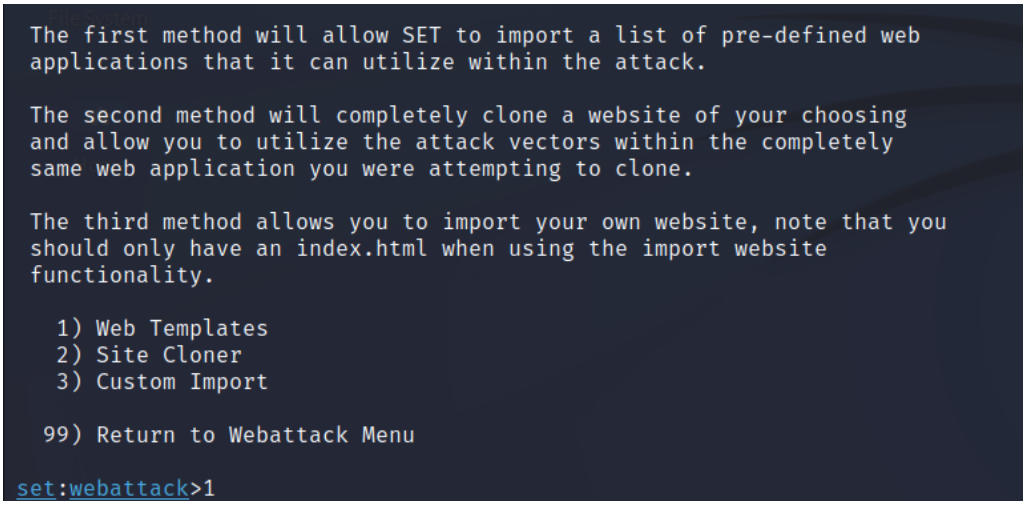
Open Kali linux

Go to Applications-> Social Engineering Tools-> Social Engineering Tool Kit (root)

Password for kali: kali







```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:1

_____________________________________________________

        **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config
```

```
Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

_____________________________________________________


  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [24/Nov/2022 07:46:03] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [24/Nov/2022 07:46:04] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [24/Nov/2022 07:46:14] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [24/Nov/2022 07:46:15] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [24/Nov/2022 07:46:15] "GET /favicon.ico HTTP/1.1" 404 -
```

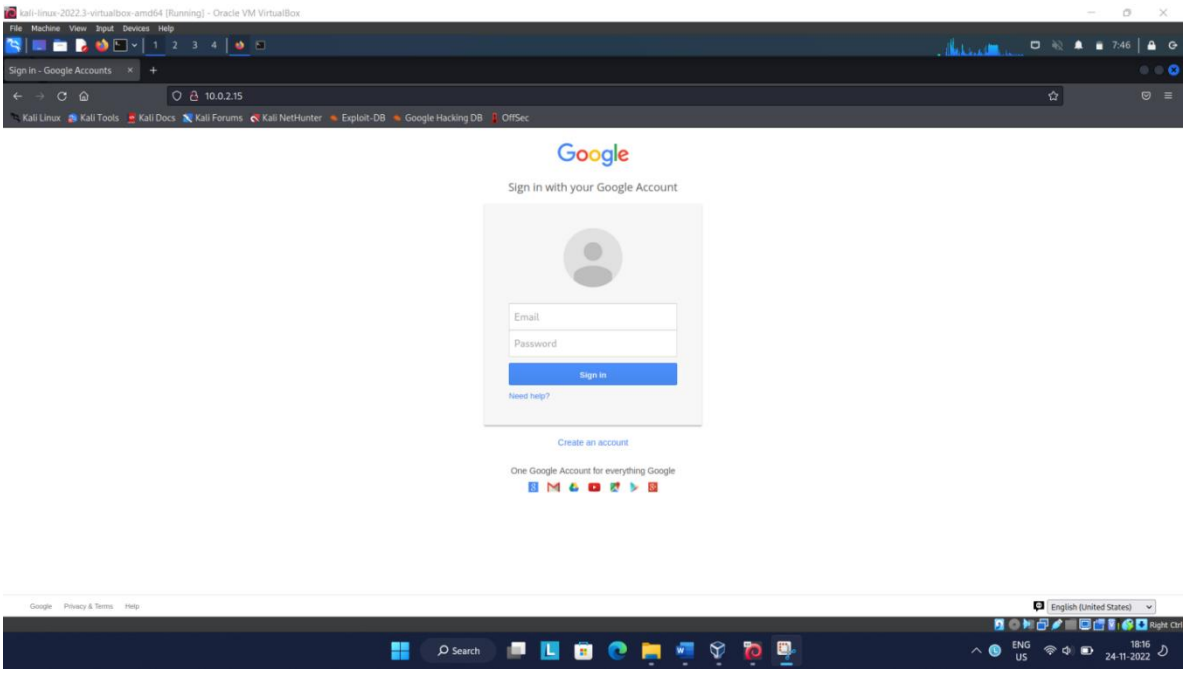


Image 1: cloned Google Sign In page

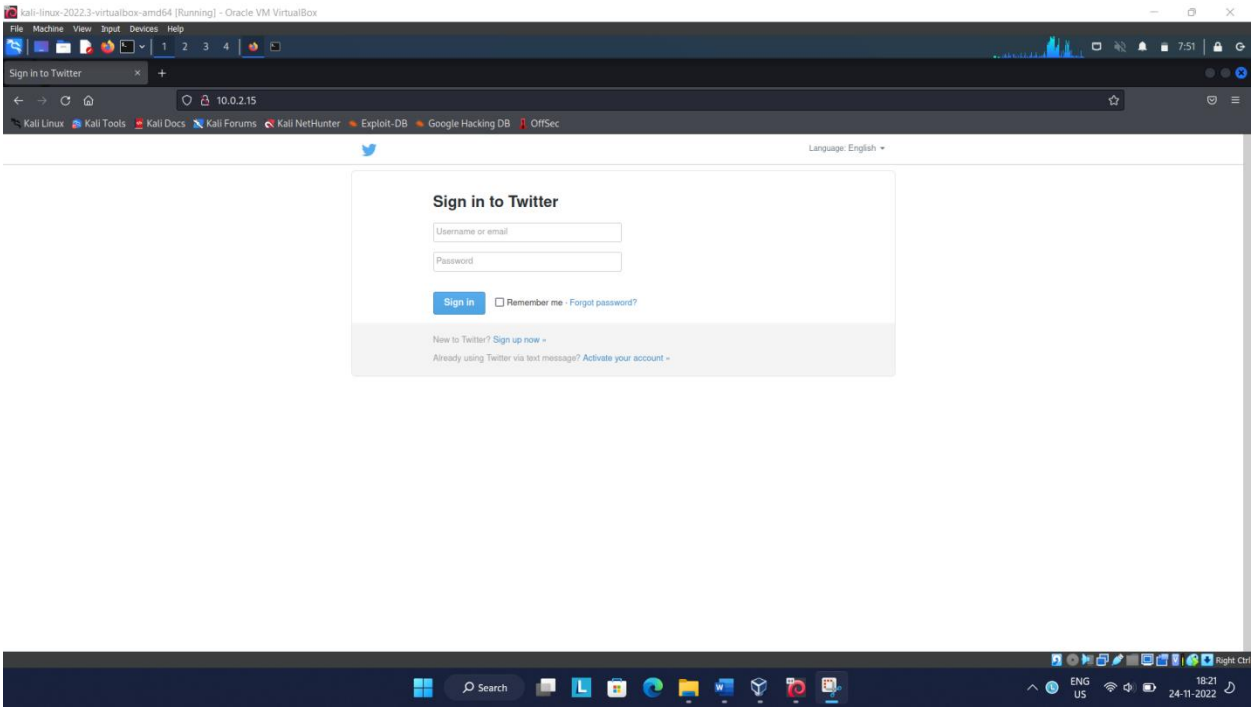


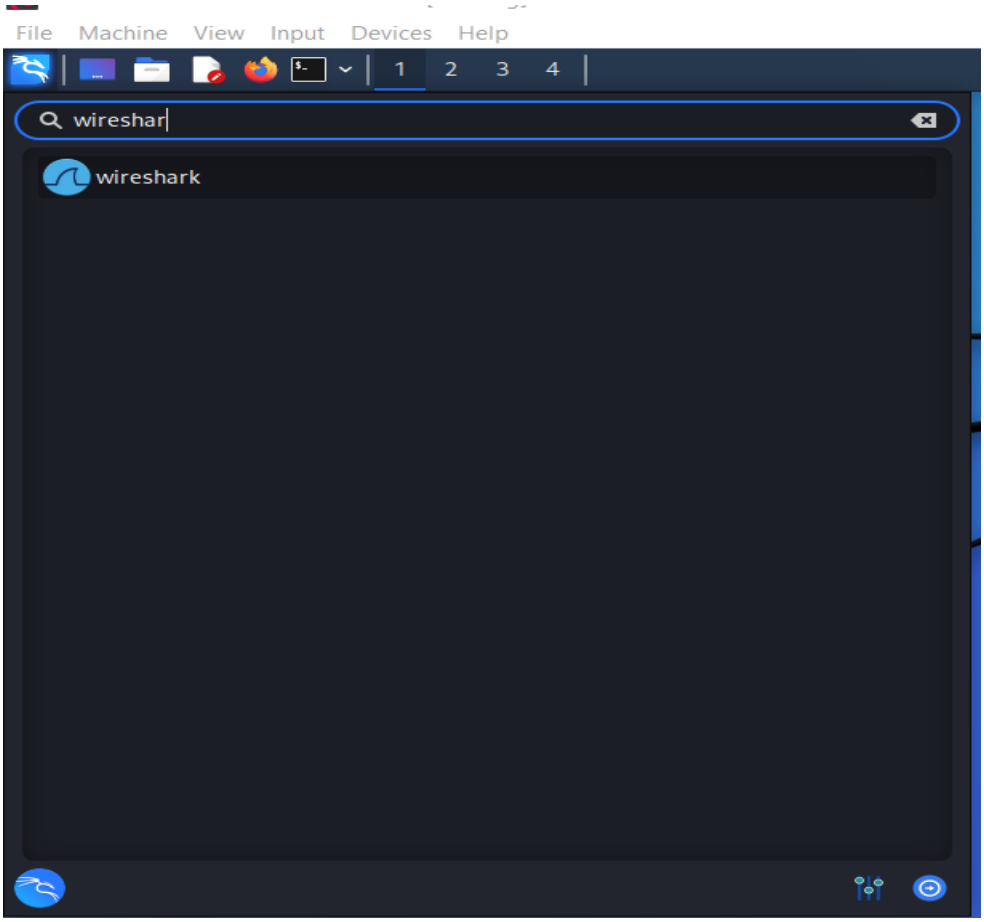
Image 2: Cloned Twitter Sign In page

Termwork - 05

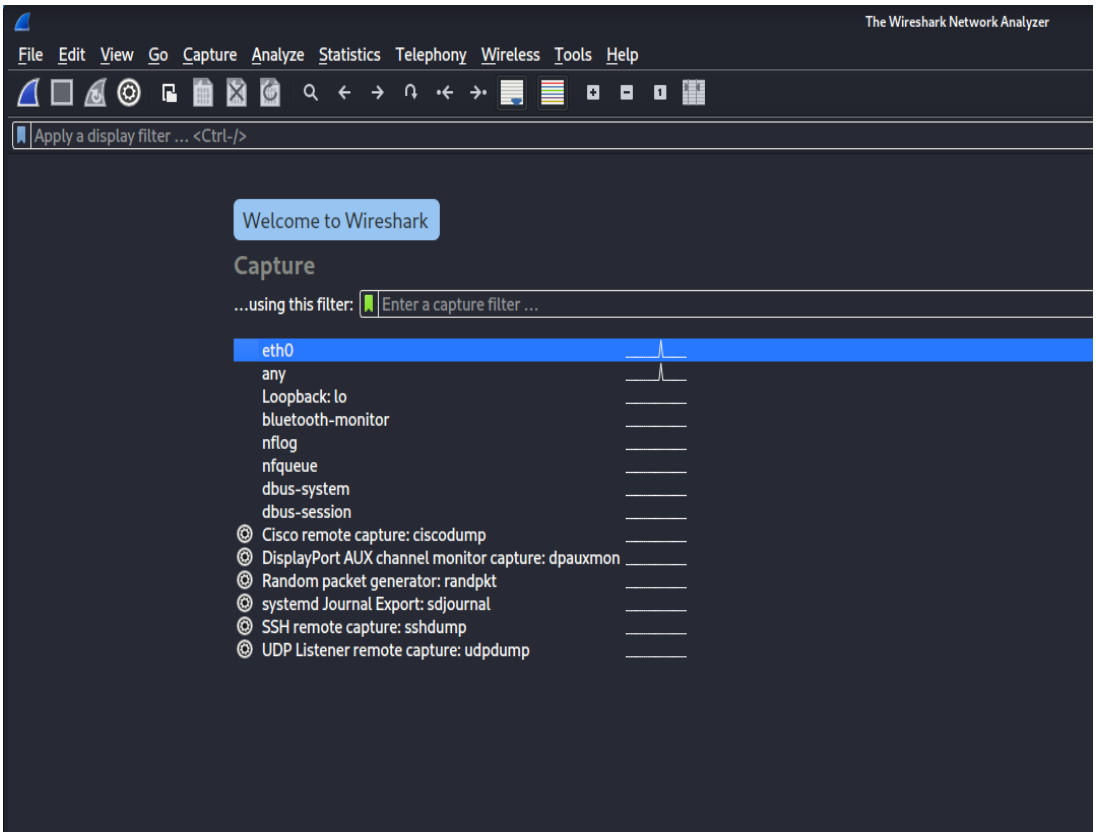
Steps in capturing packets in wireshark

1. Open wireshark and double click on any interface to start the packet capture process
2. Open browser and enter any websites fully qualified domain name in the browser address bar and hit enter.
3. After site is fully loaded , stop the capturing process in wireshark
4. Type the following in, apply the filter column and hit enter

   Tcp.flags.fin == 1 &&tcp.flags.ack == 1
5. Select any one of this and hover on the conversion filter and select tcp. Once done geeksforgeeks.com /wireshark tool

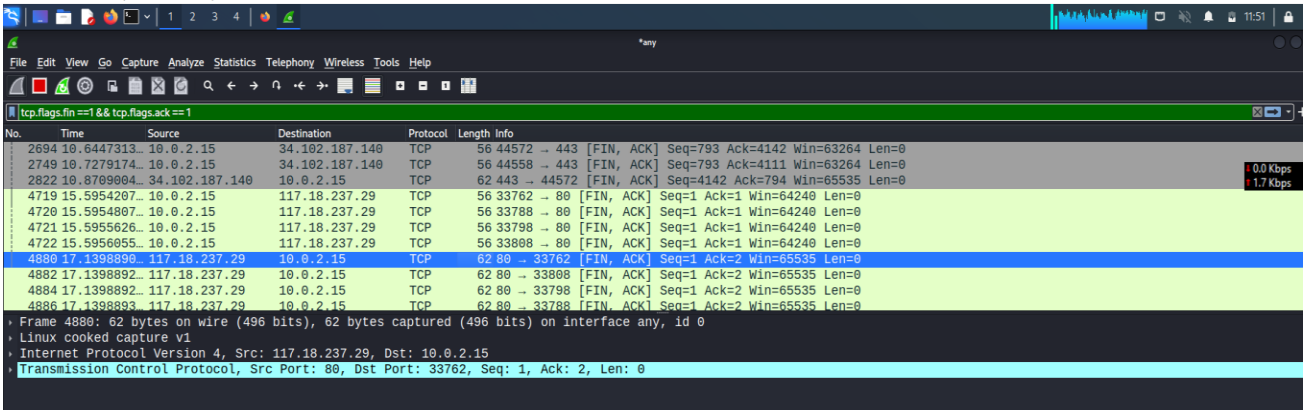


Search for wireshark in kali application



Click on Any

Open firefox and search any website



Wireshark starts capturing packets and we can apply filters (to know desired packets we required)